УНИВЕРСИТЕТ СИНЕРГИЯ

КАФЕДРА УПРАВЛЕНИЯ ЧЕЛОВЕЧЕСКИМИ РЕСУРСАМИ

УПРАВЛЕНИЕ КАДРОВОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

Для программ бакалавриата

Алавердов Ашот Робертович

Заведующий кафедрой управления человеческими ресурсами, доктор экономических наук, профессор

Контакты: alaverdov@bk.ru

ИНФОРМАЦИЯ НА ПЕРВОЙ ЛЕКЦИИ

Информация о преподавателе:

Алавердов Ашот Робертович, д.э.н., профессор, зав. кафедрой УЧР.

Сфера научно-практических интересов:

- HR-менеджмент в банковском секторе экономики;
- HR-менеджмент в малом предпринимательстве;
- управление безопасностью организации по кадровому направлению деятельности;
- антикризисное управление персоналом.

Контакты:

- e-mail: alaverdov@bk.ru;
- координаты кафедры: здание Университета у м. Семеновская, офис 405а;
- График консультаций: среда, 18-30 : 19-00, кафедра УЧР

Информация о дисциплине:

Полное наименование: Управление кадровой безопасностью организации.

Количество аудиторных часов: 32 часа (8 занятий) : 32 часа лекций + экзамен (04.06.2017).

Учебная программа дисциплины размещена в личном кабинете обучающегося.

Базис дисциплины (объем теоретических знаний, в обязательном порядке подлежащий усвоению студентом и минимально необходимый для получения им положительной оценки) – рассматривается на следующих слайдах.

Базовый учебник: Алавердов А.Р. Управление кадровой безопасностью организации: учебник. – М.: Издательство «Маркет ДС», 2008 (Университетская серия). **ПРИОБРЕТЕНИЕ И НАЛИЧИЕ УЧЕБНИКА НА ВСЕХ ВИДАХ АУДИТОРНЫХ ЗАНЯТИЙ ЯВЛЯЕТСЯ ОБЯЗАТЕЛЬНЫМ, ИСПОЛЬЗОВАНИЕ ЕГО НА ЭКЗАМЕНЕ НЕ ДОПУСКАЕТСЯ!**

Итоговое мероприятие: проводится в форме :

- либо устного ответа на вопросы экзаменационного билета, включающего в себя 3 вопроса (любая оценка);
- либо решения тестового задания из 2-х частей (при правильном ответе на не менее, чем 80% вопросов по части «А» и 80% вопросов по части «Б» оценка «хорошо», при правильном ответе на не менее, чем 50% вопросов по части «А» оценка «удовлетворительно»).

«БАЗИС» ДИСЦИПЛИНЫ

Тема 1. Кадровая безопасность организации как объект управления:

- понятие и актуальность обеспечения кадровой безопасности организации;
- классификация угроз кадровой безопасности организации и методов противодействия им;
- дополнительные особенности обеспечения кадровой безопасности организаций в современной России.

Тема 2. Система управления кадровой безопасностью организации:

- структура системы управления кадровой безопасностью: субъекты управления, операционные подсистемы, блок обеспечения;
- стратегические подходы к обеспечению кадровой безопасности: общая стратегия обеспечения безопасности;
- служба безопасности организации, ее функции в рамках системы, полномочия и ответственность;
- распределение полномочий и ответственности между инстанциями в системе управления кадровой безопасностью;
- методические требования к системе управления кадровой безопасностью.

Тема 3. Противодействие угрозам безопасности персонала организации:

- основные методы противодействия угрозе переманивания ведущих сотрудников;
- методы профилактики и пресечения угрозы угрозе склонения сотрудников организации к обману доверия работодателя;
- методы профилактики угрозы физической безопасности топ-менеджеров организации.

«БАЗИС» ДИСЦИПЛИНЫ

Тема 4. Противодействие угрозам информационной безопасности организации со стороны собственного персонала:

- ранжирование конфиденциальной информации;
- типовые причины реализации угроз информационной безопасности организации с участием ее сотрудников;
- формы реализации угроз информационной безопасности;
- методы реализации угроз информационной безопасности;
- специальное обучение персонала организации правилам обеспечения безопасности конфиденциальной информации;
- контроль над соблюдением сотрудниками правил обеспечения информационной безопасности организации;
- ответственность сотрудников за нарушение правил обеспечения информационной безопасности организации.

Тема 5. Противодействие угрозам имущественной безопасности организации со стороны собственного персонала:

- типовые причины реализации имущественной безопасности организации с участием ее сотрудников;
- типовые формы реализации угроз;
- организационные и технические методы защиты имущества организации;
- контроль над соблюдением сотрудниками правил обеспечения имущественной безопасности;
- ответственность сотрудников за нарушение правил обеспечения имущественной безопасности.

ТЕМЫ ДИСЦИПЛИНЫ

Тема 1. Кадровая безопасность организации как объект управления

Тема 2. Система управления кадровой безопасностью организации

Тема 3. Противодействие угрозам безопасности персонала организации

Тема 4. Противодействие угрозам информационной безопасности организации со стороны собственного персонала

Тема 5. Противодействие угрозам имущественной безопасности организации со стороны собственного персона

Тема 1.

Кадровая безопасность организации как объект управления

УЧЕБНЫЕ ВОПРОСЫ ТЕМЫ

1.1 Цель и основные элементы системы обеспечения кадровой безопасности организации, классификация возможных угроз и методов противодействия им.

1.2 Отраслевая специфика обеспечения кадровой безопасности организаций и дополнительные особенности ее в современной России.

1.3 Ошибки в стратегии HR-менеджмента, снижающие степень кадровой безопасности организации.

БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ - текущая и перспективная защищенность ее от разнообразных угроз имущественного и неимущественного характера.

ОБЩЕЕ ОГРАНИЧЕНИЕ: рассматриваемый в рамках дисциплины аспект обеспечения безопасности организации связан с защитой лишь от тех угроз, которые:

- **во-первых, определены деятельностью юридических и физических лиц, направленной на нанесение конкретной организации имущественного или неимущественного ущерба;**
- **во-вторых, связаны с функционированием только одного из направлений деятельности организации – а именно, кадрового направления.**

ПРЕДМЕТ ИЗУЧЕНИЯ: безопасность современной организации по кадровому направлению ее деятельности

ОСНОВНЫЕ ОБЪЕКТЫ ИЗУЧЕНИЯ:

- **понятие и классификация угроз безопасности организации по кадровому направлению ее деятельности;**
- **общее понятие и основы методологии менеджмента безопасности, его современная отечественная и отраслевая специфика;**
- **распределение функций, полномочий и ответственности между службой безопасности, кадровой службой и руководителями подразделений организации;**
- **стратегические подходы к организации обеспечения безопасности организации по кадровому направлению ее деятельности;**
- **прикладные методы защиты безопасности организации от внешних и внутренних угроз ее безопасности по рассматриваемому направлению.**

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

По признаку целевой направленности угрозы выделяются:

- **угрозы безопасности сотрудников** организации;
- **угрозы безопасности организации** со стороны ее собственных сотрудников, которые по различным могут нанести ущерб ее имущественным и неимущественным интересам.

По признаку характера потерь от реализованных угроз выделяются:

- **угрозы информационной безопасности,** связанные с деятельностью персонала и реализуемые в форме разглашения конфиденциальной информации, а также искажения или уничтожения любых сведений и баз данных, используемых организацией в своей деятельности;
- **угрозы имущественной безопасности,** связанные с деятельностью персонала и реализуемые в форме хищения или умышленного повреждения (уничтожения) различных элементов имущества организации

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ по признаку ее источника (субъекта):

- **угрозы со стороны конкурентов** (причем как самой организации - работодателя, так и ее клиентов или партнеров) стремящихся к усилению собственных позиций на соответствующем рынке путем использования методов недобросовестной конкуренции, например, деловой разведки, переманивания высококвалифицированных сотрудников, дискредитации соперника в глазах партнеров и государства;
- **угрозы со стороны криминальных структур и отдельных злоумышленников,** стремящихся к достижению собственных целей, находящихся в противоречии с интересами конкретной организации - работодателя или ее клиентов, например, захвату контроля над ним, хищению имущества, нанесению иного ущерба;
- **угрозы со стороны государства** в лице уполномоченных надзорных, регулирующих, фискальных и правоохранительных органов, деятельность которых в некоторых случаях может вызывать угрозы по кадровому направлению работы коммерческих организаций;
- **угрозы со стороны сотрудников организации,** осознанно или в силу общей безответственности наносящих ущерб ее безопасности ради достижения личных целей, например, минимизации трудовых усилий, улучшения материального положения, карьерного роста, мщения работодателю за реальные или мнимые обиды и т.п.

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

По экономическому характеру угрозы выделяются:

- **угрозы материального характера,** наносящие организации прямой и легко исчисляемый финансовый ущерб,
- **угрозы нематериального характера,** точный размер ущерба от реализации которых обычно невозможно точно определить

По вероятности практической реализации угрозы выделяются:

- **потенциальные угрозы,** практическая реализация которых на конкретный момент имеет лишь вероятностный характер;
- **реализуемые угрозы,** негативное воздействие которых на деятельность субъекта управления находится в конкретный момент в различных стадиях развития;
- **реализованные угрозы,** негативное воздействие которых уже закончилось и ущерб фактически нанесен.

КЛАССИФИКАЦИЯ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

по признаку времени их реализации:

- **профилактические или превентивные методы,** которые используются для предотвращения потенциальных угроз или на стадии их фактического зарождения;
- **пресекающие или отражающие методы,** которые используются для противодействия уже реализуемым угрозам с целью полного предотвращения или минимизации связанного с ними ущерба;
- **карающие или репрессивные методы,** которые используются для наказания виновников уже реализованных угроз и имеют своей целью не столько возмещение уже нанесенного организации ущерба, сколько предупреждение реализации аналогичных угроз в дальнейшем.

КЛАССИФИКАЦИЯ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

по признаку характера их действия:

- **методы административного характера,** предполагающие принятие руководством организации тех или иных административных решений, направленных либо на профилактику потенциальных угроз, либо на наказание их виновников;

- **методы экономического характера,** либо создающие необходимую мотивацию у сотрудников как потенциальных объектов угроз, либо реализуемые в виде санкций к сотрудникам как субъектам угроз;

- **методы психологического характера,** используемые преимущественно для профилактики возможных угроз и имеющие как коллективную, так и индивидуальную направленность.

КЛАССИФИКАЦИЯ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

по признаку степени легитимности:

- **методы легитимного характера,** реализация которых не противоречит не только действующему законодательству, но и нормам предпринимательской этики в области трудовых и конкурентных отношений;

- **методы нелегитимного характера,** реализация которых всегда противоречит нормам предпринимательской этики, реже предполагает определенные нарушения действующего законодательства, не связанные с привлечением виновных к уголовной ответственности;

- **криминальные методы,** факт реализации которых всегда предполагает привлечение виновных к уголовной ответственности.

ОТРАСЛЕВАЯ СПЕЦИФИКА ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

РЕАЛЬНЫЙ СЕКТОР ЭКОНОМИКИ:

ПРИОРИТЕТНЫЕ СУБЪЕКТЫ УГРОЗ:

- собственные сотрудники;
- конкуренты

ПРИОРИТЕТНЫЕ ОБЪЕКТЫ УГРОЗ:

- товарно-материальные ценности;
- финансовые ресурсы;
- конфиденциальная технологическая и коммерческая информация

ПРИОРИТЕТНЫЕ ФОРМЫ РЕАЛИЗАЦИИ УГРОЗ:

- мелкие хищения материальных ценностей;
- финансовые злоупотребления;
- коммерческий подкуп;
- вербовка сотрудников

ОТРАСЛЕВАЯ СПЕЦИФИКА ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ТОРГОВЛЯ И БЫТОВОЕ ОБСЛУЖИВАНИЕ :

ПРИОРИТЕТНЫЕ СУБЪЕКТЫ УГРОЗ:

- собственные сотрудники;
- конкуренты;
- криминал;
- государственные фискальные органы

ПРИОРИТЕТНЫЕ ОБЪЕКТЫ УГРОЗ:

- товарно-материальные ценности;
- денежные средства;
- конфиденциальная финансовая коммерческая информация

ПРИОРИТЕТНЫЕ ФОРМЫ РЕАЛИЗАЦИИ УГРОЗ:

- мелкие хищение товаров и денежных средств;
- финансовые злоупотребления;
- разглашение конфиденциальной информации;
- соучастие в кражах и ограблениях;
- покушения на собственников и менеджеров

ОТРАСЛЕВАЯ СПЕЦИФИКА ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ
ФИНАНСОВЫЙ СЕКТОР ЭКОНОМИКИ

ПРИОРИТЕТНЫЕ СУБЪЕКТЫ УГРОЗ:

- собственные сотрудники;
- конкуренты клиентов;
- собственные конкуренты;
- криминал;
- государственные контрольные и надзорные органы

ПРИОРИТЕТНЫЕ ОБЪЕКТЫ УГРОЗ:

- финансовая информация о клиентах;
- финансовая информация самой организации;
- безналичные денежные средства клиентов и самой организации;
- наличные денежные средства
- наиболее ценные специалисты

ПРИОРИТЕТНЫЕ ФОРМЫ РЕАЛИЗАЦИИ УГРОЗ:

- переманивание и вербовка сотрудников;
- финансовые злоупотребления (в том числе – IT);
- коммерческий подкуп;
- инициативное разглашение информации;
- соучастие в хищениях и ограблениях;
- покушения на собственников и сотрудников

ОТРАСЛЕВАЯ СПЕЦИФИКА ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

СФЕРА ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

ПРИОРИТЕТНЫЕ СУБЪЕКТЫ УГРОЗ:

- сторонние юридические и физические лица;
- криминал;
- собственные сотрудники;

ПРИОРИТЕТНЫЕ ОБЪЕКТЫ УГРОЗ:

- разрешительные и иные действия;
- конфиденциальная информация о контролируемых организациях;
- ведущие менеджеры и специалисты

ПРИОРИТЕТНЫЕ ФОРМЫ РЕАЛИЗАЦИИ УГРОЗ:

- коррупция сотрудников;
- вербовка сотрудников;
- переманивание сотрудников

ОТРАСЛЕВАЯ СПЕЦИФИКА ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

СФЕРА НАУЧНОГО ОБСЛУЖИВАНИЯ

ПРИОРИТЕТНЫЕ СУБЪЕКТЫ УГРОЗ:

- конкуренты (в том числе – зарубежные);
- собственные сотрудники

ПРИОРИТЕТНЫЕ ОБЪЕКТЫ УГРОЗ:

- научная и научно-техническая информация, составляющая коммерческую тайну;
- ведущие ученые

ПРИОРИТЕТНЫЕ ФОРМЫ РЕАЛИЗАЦИИ УГРОЗ:

- вербовка сотрудников;
- переманивание сотрудников конкурентами

ОТРАСЛЕВАЯ СПЕЦИФИКА ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ВОЕННО-ПРОМЫШЛЕННЫЙ КОМПЛЕКС

ПРИОРИТЕТНЫЕ СУБЪЕКТЫ УГРОЗ:

- зарубежные конкуренты;
- иностранные спецслужбы;
- собственные сотрудники

ПРИОРИТЕТНЫЕ ОБЪЕКТЫ УГРОЗ:

- научно-техническая информация;
- технологическая информация
- ведущие специалисты

ПРИОРИТЕТНЫЕ ФОРМЫ РЕАЛИЗАЦИИ УГРОЗ:

- вербовка сотрудников;
- подкуп сотрудников;
- выведование информации;
- переманивание ведущих специалистов

ОТЕЧЕСТВЕННАЯ СПЕЦИФИКА ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ОБЪЕКТИВНЫЕ ФАКТОРЫ:

- специфическая трудовая ментальность россиян;
- недостатки действующего законодательства в части защиты интересов частного предпринимательства;
- высокий удельный вес «теневой» и криминальной экономики

СУБЪЕКТИВНЫЕ ФАКТОРЫ:

- ориентация собственников или топ менеджмента организации на активное использование методов недобросовестной конкуренции;
- низкая степень социальной ориентации кадровой политики организации;
- неэффективная система HR-менеджмента в организации;
- недостаточная компетентность руководителей среднего и нижнего звена в области экономического и психологического аспектов управления персоналом

ОШИБКИ В ПОЛИТИКЕ РЕГУЛИРОВАНИЯ ЧИСЛЕННОСТИ ПЕРСОНАЛА

- стратегический отказ от найма молодых специалистов;
- стратегическая ориентация на активное использование труда нелегальных мигрантов;
- стратегическая ориентация на активное использование механизма аутстаффинга (лизинга персонала);
- стратегическая ориентация на краткосрочные трудовые договора;
- стратегическая ориентация на отсутствие дополнительных социальных гарантий при сокращении персонала

ОШИБКИ В ПОЛИТИКЕ РАЗВИТИЯ ПЕРСОНАЛА

- стратегическая ориентация на самоустранение от участия в повышении квалификации персонала;
- стратегическая ориентация на игнорирование требований закона перемены труда;
- стратегическая ориентация на привлечение руководителей и ведущих специалистов со стороны в ущерб подготовке собственных кадров

ОШИБКИ В ПОЛИТИКЕ МОТИВАЦИИ ПЕРСОНАЛА

- стратегическая ориентация на использование фиксированных должностных окладов, не зависящих от текущих результатов труда;
- стратегическая ориентация на использование премий как инструмента мотивации отсутствия нарушений;
- стратегическая ориентация на отказ от «механизма участия сотрудников в прибыли организации»;
- стратегическая ориентация на экономию затрат на социальную поддержку персонала;
- стратегическая ориентация на отказ от активного применения методов моральной мотивации сотрудников

ОШИБКИ В ПОЛИТИКЕ ПСИХОЛОГИЧЕСКОЙ ПОДДЕРЖКИ ПЕРСОНАЛА

- стратегическая ориентация на отказ от формализованного механизма постоянной психологической поддержки персонала;
- стратегическая ориентация на мотивацию отношений «жесткой конкуренции между сотрудниками»;
- стратегическая ориентация на отстранение службы безопасности от мониторинга состояния психологического климата в трудовом коллективе;
- стратегическая ориентация на игнорирование личностных качеств при найме и подготовке менеджеров все уровней

Задание

Сформулируйте отраслевую специфику обеспечения кадровой безопасности в сфере научного обслуживания

Домашнее задание

Определите позитивные и негативные черты национального трудового менталитета россиян, оказывающие влияние на обеспечение кадровой безопасности в отечественных условиях

Литература

1. Алавердов А.Р. Управление кадровой безопасностью организации: учебник. – М.: Маркет ДС, 2008. – 176 с. – (Университетская серия).
2. Соломанидин В.Г., Соломанидина Т.О. Кадровая безопасность компании. – М.: Альфа-Пресс, 2011. – 688с.

Тема 2.

Система управления кадровой безопасностью организации

УЧЕБНЫЕ ВОПРОСЫ ТЕМЫ:

2.1 Структура системы управления кадровой безопасностью
2.2 Стратегические подходы к обеспечению кадровой безопасности
2.3 Служба безопасности организации и ее функции в рамках системы
2.4 Распределение полномочий и ответственности между инстанциями в системе управления кадровой безопасностью
2.5 Методические требования к системе управления кадровой безопасностью и критерии оценки ее эффективности

СТРАТЕГИЯ УПРАВЛЕНИЯ – совокупность стратегических целей и подходов по данному направлению системы внутрифирменного менеджмента.

ОПЕРАЦИОННЫЕ ПОДСИСТЕМЫ – автономные элементы системы управления, направленные на решение однотипных задач по обеспечению кадровой безопасности организации.

БЛОК ОБЕСПЕЧЕНИЯ – совокупность элементов ресурсного и иного обеспечения, необходимых для эффективного функционирования системы управления

СПЕЦИФИКА СИСТЕМЫ УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

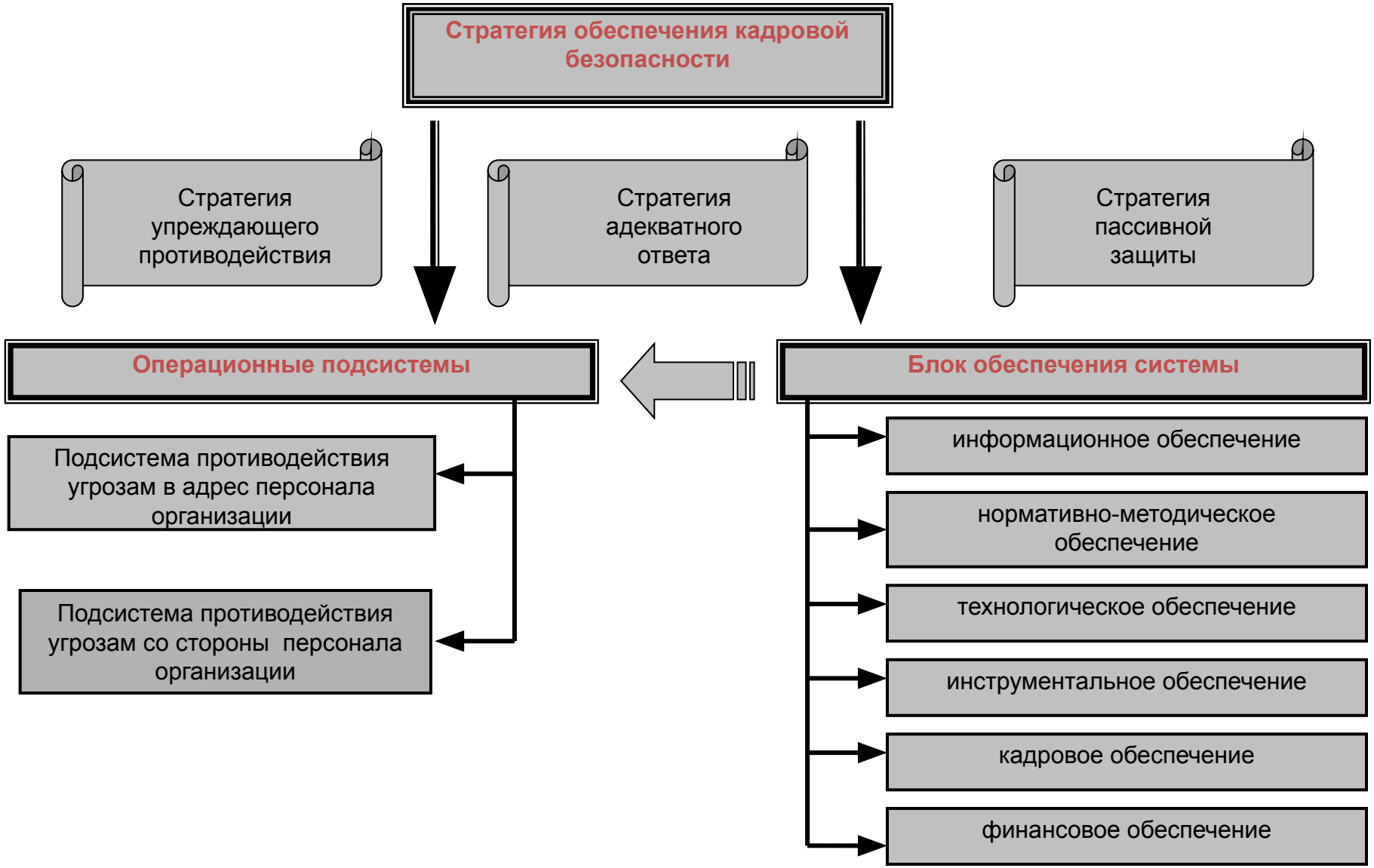
ОПРЕДЕЛЯЕТСЯ местом в комплексной системе внутрифирменного менеджмента – «стык» двух систем управления:

- **системы HR-менеджмента;**
- **системы менеджмента безопасности.**

ОПРЕДЕЛЯЕТ:

- **особенности взаимодействия между руководителями соответствующих направлений уставной деятельности организации, службой персонала и службой безопасности, руководителями прочих подразделений организации и указанными выше штабными службами;**
- **необходимость координации стратегий HR-менеджмента и менеджмента безопасности.**

2.1 Структура системы управления кадровой безопасностью



ОПЕРАЦИОННЫЕ ПОДСИСТЕМЫ СИСТЕМЫ УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

СОСТАВ ПОДСИСТЕМ:

- подсистема защиты сотрудников организации;
- подсистема защиты организации от угроз со стороны собственных сотрудников.

МЕТОДИЧЕСКИЕ ТРЕБОВАНИЯ К ПОДСИСТЕМАМ:

- подсистемы не могут содержать элементов (методов, процедур и т.п.), практическое функционирование которых может объективно затруднить эксплуатацию смежных подсистем;
- общая структура каждой из подсистем должна соответствовать следующей типовой схеме: “определение целей процесса - планирование и организация процесса - оперативное управление процессом - оценка результатов процесса путем сопоставления их с ранее запланированными целями”;
- формализованное закрепление функций, связанных с эксплуатацией подсистем, за соответствующими руководителями и специалистами, как штабных, так и производственных подразделений организации, включая и механизм персонифицированной ответственности за их выполнение.

БЛОК ОБЕСПЕЧЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ
ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

- используемые в рамках системы методы и конкретные процедуры получения субъектами управления необходимой первичной информации;

- формализованные каналы прохождения информации в рамках системы, которые определяют маршрут движения информации по инстанциям (принципиальная схема: «от кого - кому - в каких объемах и форме - в какие сроки»);

- базы данных, связанных с любыми проблемами внутренней и внешней кадровой безопасности, которые накапливаются и обновляются в течение всего периода функционирования организации и используются при формировании управленческих решений любого уровня.

БЛОК ОБЕСПЕЧЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

ВНЕШНЕЕ ОБЕСПЕЧЕНИЕ: совокупность законодательных и подзаконных актов, обязательных для исполнения всеми работодателями:

- Конституция РФ;
- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (в ред. от 05.10.2015);
- Закон РФ «О безопасности» от 28.12.2010 №390-ФЗ (в ред. от 05.10.2015);
- Закон РФ «О частной детективной и охранной деятельности в РФ» от 11.03.1992 №2487-1 (в ред. от 13.07.2015);
- Закон РФ «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ (в ред. от 31.12.2014);
- Закон РФ "О государственной тайне" от 21.07.1993 № 5485-1 (в ред. от 08.03.2015);
- Закон РФ «О коммерческой тайне» от 29.07.2004 № 98-ФЗ (в ред. от 12.03.2014);
- Закон РФ «О персональных данных» от 27.07.2006 № 152-ФЗ (в ред. от 01.09.2015)

БЛОК ОБЕСПЕЧЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ
НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

ВНУТРЕННЕ ОБЕСПЕЧЕНИЕ: совокупность регламентов и других нормативно-методических документов конкретной организации:

- Положения о службе персонала;
- Положения о службе безопасности;
- должностные инструкции топ-менеджеров, возглавляющих соответствующие направления деятельности организации, специалистов кадровой службы и службы безопасности, а также руководителей всех структурных подразделений;
- инструкции, определяющие порядок работы с конфиденциальной информацией (базами данных, документами на бумажных носителях, правила проведения конфиденциальных переговоров и т.п.);
- инструкции, определяющие порядок работы с имущественными комплексами организации в части обеспечения их сохранности;
- рекомендации сотрудникам организации в рассматриваемой области (например, «Памятка молодому специалисту»).

УНИВЕРСИТЕТ СИНЕРГИЯ

БЛОК ОБЕСПЕЧЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ
ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Совокупность формализованных технологий обеспечения безопасности организации от различных видов кадровых угроз, четко определяющих:

- ***непосредственных участников*** (инстанции и рабочие места, принимающие участие в описываемой операции по защите от конкретной угрозы);
- ***управленческие процедуры*** (мероприятия, осуществляемые в рамках операции);
- ***типовые сроки*** по операции в целом и каждой управленческой процедуре в отдельности;
- ***ответственность участников*** за нарушение описываемой технологии.

ИНСТРУМЕНТАЛЬНОЕ ОБЕСПЕЧЕНИЕ - совокупность прикладных методов управления, используемых в рамках системы.

ФИНАНСОВОЕ ОБЕСПЕЧЕНИЕ - совокупность финансовых ресурсов, выделяемых на поддержание и развитие рассматриваемого направления (приобретение спецоборудования, зарплата персонала, оплата информации и т.п.).

БЛОК ОБЕСПЕЧЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

КАДРОВОЕ ОБЕСПЕЧЕНИЕ

Во-первых, полностью укомплектованный штат штабных служб, ответственных за управление кадровой безопасностью организации, и включающий в себя три квалификационные категории работников:

- ***менеджеры***, т.е. руководители различного уровня – от возглавляющего соответствующее направление вице-президента организации до бригадира смены охранников;
- ***эксперты***, т.е. высококвалифицированные сотрудники, специализирующиеся на определенных направлениях обеспечения кадровой безопасности (аналитики, разработчики специальных программных средств и т.п.), но не выполняющие при этом прямых управленческих функций;
- **исполнители** (охранники, ремонтники спецоборудования и др.).

Во-вторых, руководители всех структурных подразделений организаций, прошедшие специальную подготовку в области обеспечения кадровой безопасности на уровне своих подразделений.

СТРАТЕГИЯ УПРЕЖДАЮЩЕГО ПРОТИВОДЕЙСТВИЯ УГРОЗАМ

ОБЩИЕ ЦЕЛИ И ПРИНЦИПЫ:

- приоритет профилактических методов противодействия возможным угрозам;
- «цель оправдывает средства», т.е. возможность применения нелегитимных методов.

ПРЕИМУЩЕСТВА:

- возможность эффективного решения возникающих проблем практически без участия государства;
- возможность обеспечения эффективной поддержки других направлений внутрикорпоративного менеджмента.

НЕДОСТАТКИ:

- высокая вероятность конфликтов с действующим законодательством, конкурентами;
- необходимость дорогостоящей ресурсной поддержки.

РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ:

- корпорации, занимающие лидирующие позиции на обслуживаемом высоко конкурентом рынке;
- высокорентабельные организации, работающие в условиях жесткого прессинга со стороны конкурентов или криминальных структур.

СТРАТЕГИЯ ПАССИВНОГО ПРОТИВОДЕЙСТВИЯ УГРОЗАМ

ОБЩИЕ ЦЕЛИ И ПРИНЦИПЫ:

- приоритетная ориентация на защиту со стороны государства в лице правоохранительных и судебных органов;
- минимизация собственных затрат.

ПРЕИМУЩЕСТВА:

- минимальные затраты на практическую реализацию стратегии;
- отсутствие угрозы конфликтов и связанных с ними проблем в отношениях с конкурентами, государством, собственным персоналом.

НЕДОСТАТКИ:

- полная зависимость безопасности организации от эффективности деятельности правоохранительных органов государства;
- ориентация на методы противодействия уже реализованным угрозам, которые являются менее эффективными по сравнению с профилактическими и пресекающими.

РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ:

- для небольших организаций, работающих на наименее конкурентных рынках;
- для организаций, находящихся в собственности государства или под непосредственным патронажем органов государственного управления.

СТРАТЕГИЯ АДЕКВАТНОГО ПРОТИВОДЕЙСТВИЯ УГРОЗАМ

ОБЩИЕ ЦЕЛИ И ПРИНЦИПЫ:

- предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз;
- в порядке исключения допускается использование и не полностью легитимных методов, но лишь в отношении тех конкурентов или иных источников угроз, которые первыми применили подобные методы.

Данный вариант является ***компромиссом*** между первым и вторым вариантом, смягчая их радикальные недостатки, но и не позволяя в полной мере использовать их преимущества.

РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ: для большинства современных работодателей.

ФАКТОРЫ, ОПРЕДЕЛЯЮЩИЕ ВЫБОР КОНКРЕТНОГО ВАРИАНТА СТРАТЕГИИ ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

- отрасль или сфера деятельности организации, определяющая, во-первых, общий уровень конкурентности соответствующих рынков и, во-вторых, заинтересованность государства в развитии отрасли, а значит и в поддержке относящихся к ней хозяйствующих субъектов;
- степень агрессивности конкурентной стратегии организации, определяющая различную вероятность угроз ее безопасности со стороны конкурентов;
- степень легитимности бизнеса организации, определяющая различную вероятность угроз ее безопасности со стороны криминала и соответствующих государственных органов;
- финансовые возможности организации по обеспечению безопасности;
- квалификация персонала службы безопасности, что прямо связано с предыдущим фактором;
- наличие поддержки со стороны органов государственной власти, следовательно, возможность привлечения к обеспечению безопасности организации правоохранительных органов и спецслужб.

ОБЩИЕ ФУНКЦИИ, ПОЛНОМОЧИЯ И ОТВЕТСТВЕННОСТЬ СЛУЖБЫ БЕЗОПАСНОСТИ

- разработка и практическая реализация стратегии управления кадровой безопасностью;
- методическое руководство деятельностью других подразделений организации;
- специальное обучение персонала организации;
- общий мониторинг соответствующего направления деятельности других подразделений организации;
- организация служебных расследований;
- выполнение соответствующих заявок со стороны других подразделений, включая службу персонала;
- общая ответственность за эффективность системы управления.

СТРАТЕГИЧЕСКИЕ ПОДХОДЫ К ОРГАНИЗАЦИИ СЛУЖБЫ

ПЕРВЫЙ ПОДХОД предполагает полный отказ от услуг сторонних специализированных структур и формирование полноценной по функциям собственной службы безопасности.

Преимущества подхода:

- большая степень доверия к штатным сотрудникам;
- высокая степень мотивированности к эффективной работе.

Недостатки подхода:

- высокий уровень затрат на содержание подобной службы;
- объективные сложности с комплектацией ее высококвалифицированными сотрудниками всех необходимых специальностей.

Рекомендации по применению: для организаций, реализующих стратегию упреждающего противодействия угрозам.

СТРАТЕГИЧЕСКИЕ ПОДХОДЫ К ОРГАНИЗАЦИИ СЛУЖБЫ

ВТОРОЙ ПОДХОД предполагает минимизацию штатных сотрудников службы безопасности, с возложением основных ее функций на сторонние специализированные структуры, привлекаемые на договорной основе.

Преимущества подхода:

- меньшая капиталоемкость;
- возможность для руководства организации снять с себя ответственность за нелегитимные действия привлеченного частного агентства.

Недостатки подхода:

- меньшая степень доверия к сторонним для организации сотрудникам;
- меньшая оперативность системы управления безопасностью.

Рекомендации по применению: для организаций, реализующих стратегию пассивной защиты от угроз.

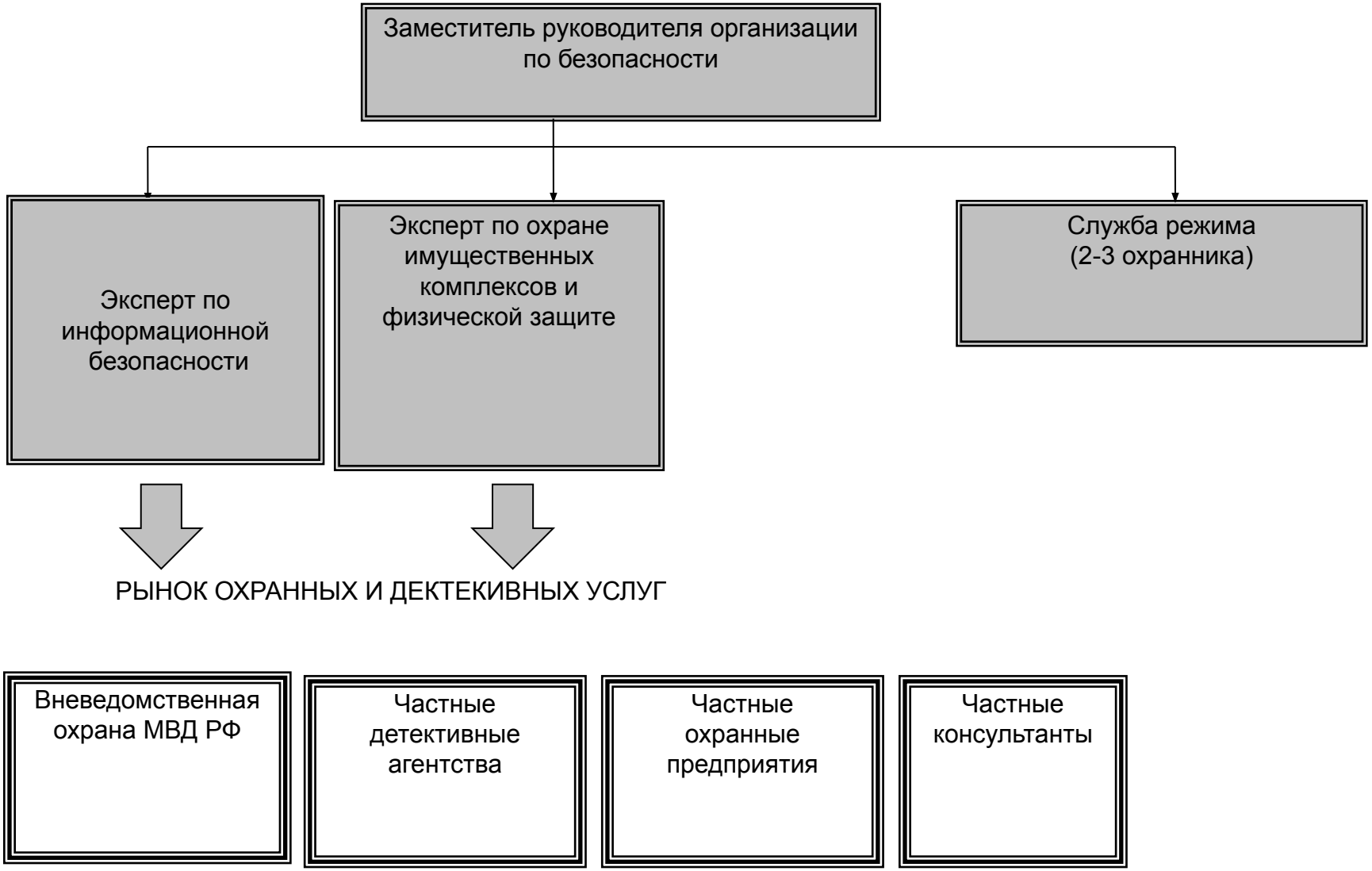
СТРАТЕГИЧЕСКИЕ ПОДХОДЫ К ОРГАНИЗАЦИИ СЛУЖБЫ

ТРЕТИЙ ПОДХОД предполагает возможность ограниченного использования услуг специализированных частных структур для выполнения локальных задач, обычно сомнительных с позиции их легитимности.

Данный вариант является ***компромиссом*** между первым и вторым вариантом, смягчая их радикальные недостатки, но и не позволяя в полной мере использовать их преимущества.

Рекомендуется для большинства современных работодателей.

2.3 Служба безопасности организации и ее функции в рамках системы



ОБЯЗАННОСТИ РУКОВОДИТЕЛЯ СЛУЖБЫ:

- формирование общей стратегии обеспечения безопасности и ее оперативная корректировка при изменении внешних или внутренних условий;
- решение текущих проблем с высшим руководством и начальниками структурных подразделений организации;
- организация взаимодействия с местными правоохранительными органами;
- формирование и контроль над исполнением целевых программ и текущих планов структурных подразделений службы безопасности, решение всех ее внутренних административных вопросов, организация ресурсного обеспечения;
- непосредственное руководство службами собственной безопасности и экспертов – консультантов

ПОЛНОМОЧИЯ РУКОВОДИТЕЛЯ СЛУЖБЫ:

- право доступа к любой конфиденциальной информации;
- право участия в совещаниях и переговорах любого уровня, где затрагиваются вопросы, представляющие потенциальную угрозу для безопасности организации (при невозможности личного участия – полный отчет или магнитофонная запись переговоров);
- право внеочередного доступа к первому руководителю организации, а в экстренной ситуации – ее основному собственнику;
- право функционального руководства и контроля деятельности других должностных лиц организации в рамках установленной компетенции

ФУНКЦИИ АНАЛИТИЧЕСКОГО ОТДЕЛА - сбор и анализ информации:

- о конкурентах в части изменений их рыночной стратегии, имеющихся ресурсов, деловых связей, используемых технологий и, естественно, прямых угрозах безопасности организации с их стороны;
- о клиентах и деловых партнерах в части, прежде всего, их коммерческой добропорядочности, финансовой надежности, планов дальнейшего сотрудничества с организацией;
- о деятельности преступных группировок, представляющих потенциальную или реальную угрозу для безопасности организации;
- о подготовке конкретных покушений на безопасность организации, а также иных, враждебных ей акций в режиме внешних угроз;
- о соблюдении в трудовых коллективах организации правил обеспечения безопасности, которые невозможно получить в ходе плановых и внезапных проверок режима;
- о сотрудниках, лояльность которых стала вызывать сомнения у непосредственного руководителя или психолога службы персонала;
- о сотрудниках, занимающих ключевые рабочие места, служебные возможности которых делают необходимым постоянный контроль;
- об общем психологическом настрое в трудовых коллективах организации, дополняющие информацию от психолога службы персонала

ФУНКЦИИ ОТДЕЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

- защита компьютерных сетей и баз данных от несанкционированного проникновения;
- защита информации на бумажных носителях, что связано, в основном с разработкой специальных правил работы с документацией и ее хранения;
- защита устной информации от перехвата с использованием специальных технических средств

ФУНКЦИИ ОТДЕЛА ФИЗИЧЕСКОЙ ЗАЩИТЫ:

- обеспечение личной безопасности руководителей и собственников организации;
- обеспечение охраны имущественных комплексов организации и иные общережимные мероприятия

ФУНКЦИИ ОТДЕЛА СОБСТВЕННОЙ БЕЗОПАСНОСТИ:

- участие в разработке внутренних регламентов службы безопасности, определяющих правила поведения ее сотрудников при исполнении служебных обязанностей и в быту;
- профилактический контроль над деятельностью всех сотрудников службы безопасности в части исполнения указанных выше правил;
- проведение служебных расследований в отношении сотрудников других подразделений службы безопасности, допустивших нарушения при исполнении своих обязанностей или поставивших под сомнение свою лояльность работодателю

КОНТРОЛЬ НАД ДЕЯТЕЛЬНОСТЬЮ СЛУЖБЫ БЕЗОПАСНОСТИ

- ***со стороны правоохранительных органов*** (отсутствие нарушений законодательства при исполнении службой безопасности своих функций);
- ***со стороны руководства организации*** (эффективность исполнения установленных ей функций и отсутствие фактов превышения установленных полномочий);
- ***в режиме внутреннего контроля в рамках самой службы*** (по аналогу с деятельностью службы собственной безопасности в государственных правоохранительных органах).

ВЗАИМОДЕЙСТВИЕ СЛУЖБЫ БЕЗОПАСНОСТИ С ДРУГИМИ ИНСТАНЦИЯМИ ОРГАНИЗАЦИИ

ВЗАИМОДЕЙСТВИЕ СО СЛУЖБОЙ МАРКЕТИНГА:

- совместное изучение и анализ конкурентов, подготовка аналитических обзоров и рекомендаций для руководства и подразделений организации;
- выполнение специальных поручений по сбору дополнительной информации об отдельных клиентах и партнерах организации (в том числе и потенциальных).

ВЗАИМОДЕЙСТВИЕ СО СЛУЖБОЙ ПЕРСОНАЛА:

- проведение специальных проверок при найме новых сотрудников по заявке со стороны службы персонала;
- участие в первичном обучении вновь нанятых сотрудников;
- координация действий по контролю над лояльностью персонала и соблюдением им правил обеспечения безопасности работодателя.

ВЗАИМОДЕЙСТВИЕ СЛУЖБЫ БЕЗОПАСНОСТИ С ДРУГИМИ ИНСТАНЦИЯМИ ОРГАНИЗАЦИИ

ВЗАИМОДЕЙСТВИЕ С ФИНАНСОВОЙ СЛУЖБОЙ:

- передача и обоснование заявок на финансовые ресурсы, необходимые для подразделения, отчеты об использовании выделенных средств;
- совместное расследование фактов нарушений корпоративной финансовой дисциплины (в случае прямых хищений и растрат).

ВЗАИМОДЕЙСТВИЕ СО СЛУЖБОЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ:

- совместные действия по защите компьютерных сетей организации от несанкционированного проникновения и повреждения;
- при разработке службой компьютерного обеспечения новых программных продуктов – проверка их защищенности от соответствующих угроз.

2.4 Распределение полномочий и ответственности между инстанциями в системе управления кадровой безопасностью

ТОП МЕНЕДЖМЕНТ:

- выбор базовой концепции организации внутрифирменных трудовых отношений;
- утверждение общей стратегии управления безопасностью;
- выделение необходимых ресурсов;
- контроль над общей эффективностью системы.

СЛУЖБА БЕЗОПАСНОСТИ:

- разработка и практическая реализация стратегии управления кадровой безопасностью;
- методическое руководство деятельностью других подразделений организации;
- специальное обучение персонала организации;
- общий мониторинг соответствующего направления деятельности других подразделений организации;
- организация служебных расследований;
- выполнение соответствующих заявок со стороны других подразделений, включая службу персонала;
- общая ответственность за эффективность системы управления.

2.4 Распределение полномочий и ответственности между инстанциями в системе управления кадровой безопасностью

СЛУЖБА ПЕРСОНАЛА:

- реализация установленных функций по обеспечению должной ответственности и лояльности персонала;
- общая ответственность за эффективное противодействие угрозе переманивания сотрудников;
- оперативное взаимодействие со службой безопасностью.

РУКОВОДИТЕЛИ ПРОЧИХ ПОДРАЗДЕЛЕНИЙ:

- текущая работа по специальному обучению своих подчиненных;
- текущий контроль над соблюдением подчиненными правил обеспечения безопасности;
- оперативное взаимодействие со службой безопасностью.

Методические требования к системе управления кадровой безопасностью:

- системный подход к проблеме обеспечения кадровой безопасности;
- приоритет мероприятий по предотвращению потенциальных угроз (т. е. методов профилактического характера);
- обеспечение приоритетной защиты конфиденциальной информации и лишь затем иных объектов потенциальных угроз;
- непосредственное участие в обеспечении кадровой безопасности организации всех ее должностных лиц в рамках установленной им компетенции и ответственности;
- обеспечение взаимодействия системы управления кадровой безопасностью с другими направлениями менеджмента;
- соразмерность затрат на обеспечение кадровой безопасности организации реальному уровню угроз;
- формализованное закрепление не только функциональных обязанностей, но и полномочий (предела компетенции) службы безопасности.

Критерии оценки эффективности системы управления кадровой безопасностью:

- динамика текучести кадров в форме инициативных увольнений сотрудников, в т.ч. – ушедших на работу к непосредственным конкурентам;
- общее количества выявленных угроз, с дифференциацией на угрозы, пресеченные в полном объеме, пресеченные частично, негативно реализованные в полном объеме (в сравнении с предыдущими периодами);
- прямой финансовый ущерб, нанесенный организации в результате частично и полностью реализованных угроз;
- потенциальный ущерб, который могли бы нанести организации полностью или частично пресеченные угрозы;
- результаты реализации плановых профилактических мероприятий;
- отсутствие обоснованных претензий к службе безопасности со стороны правоохранительных органов, собственных подразделений и отдельных сотрудников.

Задание

Определите и обоснуйте - какой из стратегических подходов к обеспечение кадровой безопасности в наибольшей степени подходит для лидирующего на рынке банка?

Домашнее задание

Определите, какие элементы входят в состав информационного обеспечения системы кадровой безопасности современной организации?

Литература

1. Алавердов А.Р. Управление кадровой безопасностью организации: учебник. – М.: Маркет ДС, 2008. – 176 с. – (Университетская серия).
2. Соломанидин В.Г., Соломанидина Т.О. Кадровая безопасность компании. – М.: Альфа-Пресс, 2011. – 688с.

Тема 3.

Противодействие угрозам безопасности персонала организации

УЧЕБНЫЕ ВОПРОСЫ ТЕМЫ

3.1 Противодействие угрозе переманивания сотрудников организации

3.2 Противодействие угрозе склонения сотрудников к нелояльному поведению в отношении работодателя

3.3 Противодействие угрозе покушений на сотрудников организации

СУБЪЕКТЫ УГРОЗЫ:

- для любых организаций кроме органов государственного управления – конкуренты;
- для государственных органов – подведомственные или подконтрольные ими коммерческие структуры.

ОБЪЕКТЫ УГРОЗЫ:

- менеджеры высшего и среднего звена;
- ведущие специалисты;
- высококвалифицированные работники, представители рабочих профессий.

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗЫ:

- предложение лучших условий найма;
- предложение о параллельном решении жизненно важной для человека проблемы (например, выдача кредита на покупку квартиры, оплата дорогостоящего лечения близкого родственника и т.п.);
- шантаж в форме угрозы передачи работодателю или правоохранительным органам компрометирующей сотрудника информации (как наименее распространенная форма).

ОСНОВНОЙ ПРИЧИНОЙ РЕАЛИЗАЦИИ УГРОЗЫ

выступает недовольство переманиваемого сотрудника:

- экономическими или социальными условиями найма, включая их юридическое оформление (например, использование в отношении его «серых схем» оплаты труда);
- перспективами собственного профессионального и карьерного роста;
- факторами, характеризующими самого работодателя (устойчивость положения на рынке, масштаб и степень легитимности бизнеса, организационно-правовой статус и т.п.);
- общим состоянием психологического климата в организации (например, из-за реализуемой работодателем политики поощрения активной внутрифирменной конкуренции между сотрудниками);
- отношениями с непосредственным руководителем (чаще – из-за отсутствия у него необходимых личностных качеств, реже – в силу объективной психологической несовместимости);
- отношениями с коллегами по работе.

НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ УГРОЗЫ ДЛЯ ОРГАНИЗАЦИИ РАБОТОДАТЕЛЯ:

- **ухудшение качества собственного человеческого капитала с одновременным улучшением его у конкурирующей организации;**
- **высокая вероятность разглашения конфиденциальной информации сотрудником, перешедшим на работу к конкуренту;**
- **в некоторых случаях – возможность потери части клиентов, ушедших на обслуживание в конкурирующую организацию вслед за курировавшим их специалистом.**

ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗЕ реализуется преимущественно в рамках системы персонального менеджмента (а не системы менеджмента безопасности) на основе следующих методических принципов и распределения ответственности между инстанциями:

- ***топ-менеджеры*** **(в сферах среднего и малого бизнеса – собственники) несут ответственность за выбор кадровой стратегии, основанной на требованиях доктрины «развития человеческого капитала организации», игнорирование которых делает любую организации изначально уязвимой к рассматриваемой угрозе;**
- ***кадровая служба*** **несет общую ответственность за обеспечение безопасности наиболее ценных сотрудников организации от переманивания конкурентами путем внедрения в практику персонального менеджмента прикладных механизмов и технологий, направленных на сокращение до минимума перечня возможных причин инициативных увольнений;**
- ***служба безопасности*** **привлекается к отражению рассматриваемой угрозы только в случае появления на соответствующем рынке труда «кадрового агрессора», т.е. конкурирующей организации, целенаправленно пытающейся лишить конкретного работодателя значительной части его наиболее ценных сотрудников.**

СУБЪЕКТЫ УГРОЗЫ:

ВНЕШНИЕ:

- государство (в лице правоохранительных, фискальных и контролирующих органов);
- конкуренты (как организации – работодателя, так и ее контрагентов);
- криминальные структуры;
- индивидуально действующие злоумышленники.

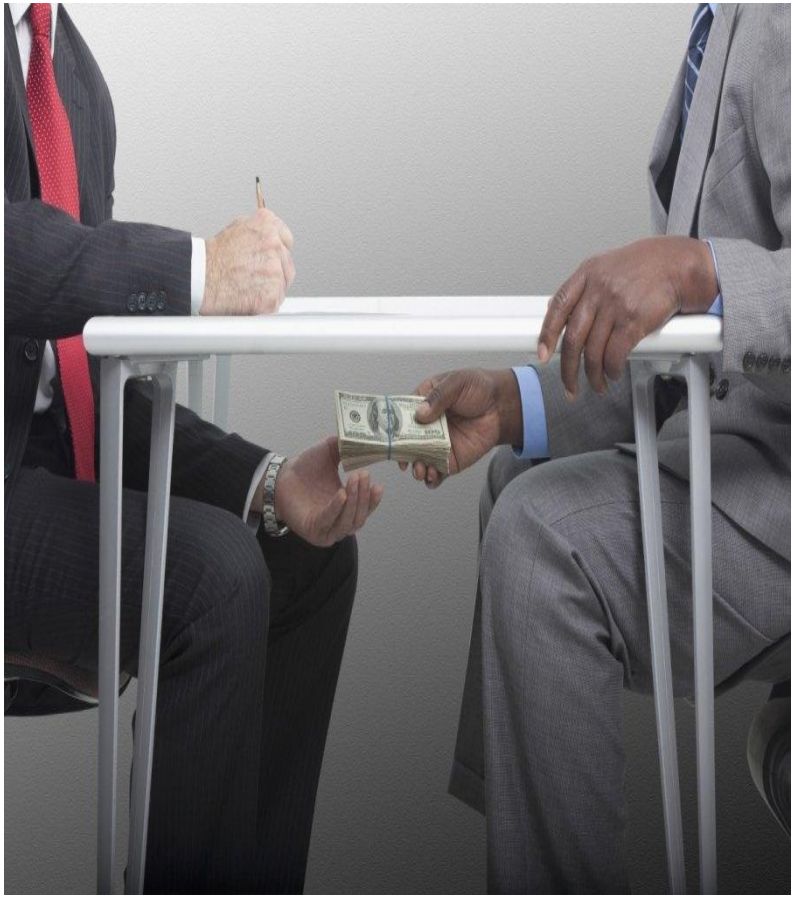
ВНУТРЕННИЕ:

- руководитель сотрудника – объекта угрозы;
- подчиненный сотрудника – объекта угрозы;
- работники подконтрольных сотруднику подразделений;
- коллеги по работе, не состоящие в отношениях соподчиненности.

ОБЪЕКТЫ УГРОЗЫ – должностные лица (реже – рядовые сотрудники) организации, занимающие рабочие места, которые обеспечивают доступ:

- к конфиденциальной информации;
- к управлению денежными средствами и ликвидными товарно-материальными ценностями, а также к хранению их;
- к реализации функций управления, регулирования и надзора.

ИНСТРУМЕНТЫ РЕАЛИЗАЦИИ УГРОЗЫ:



- **прямой или косвенный подкуп;**
- **предложение о трудоустройстве;**
- **шантаж;**
- **«игра» на недовольстве работодателем;**
- **прямые угрозы.**

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗЫ:

- превращение сотрудника в постоянно действующий источник утечки конфиденциальной информации;
- разовое разглашение сотрудником конфиденциальных сведений;
- соучастие сотрудника в реализации угроз в адрес работодателя со стороны третьих лиц (кража, финансовая афера, ограбление, обеспечение доступа в закрытые сети или базы данных и т.п.);
- злоупотребление сотрудником своими служебными полномочиями в интересах третьего лица – выгодоприобретателя (закупка некондиционных товарно-материальных ценностей, выдача заведомо невозвратного кредита, организация «заказных» проверок и т.п.);
- акты прямого саботажа в форме уничтожения или искажения сотрудником доверенных ему документов по заказу третьего лица.

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗЫ СКЛОНЕНИЯ СОТРУДНИКОВ К НАРУШЕНИЮ ОБЯЗАТЕЛЬСТВ ПЕРЕД РАБОТОДАТЕЛЕМ СО СТОРОНЫ ЕГО КОНКУРЕНТОВ

ОБЪЕКТ УГРОЗЫ:

сотрудники организации, имеющие доступ к конфиденциальной научной, технологической, коммерческой, финансовой или кадровой информации, а также к наиболее ценным имущественным комплексам

ЦЕЛИ РЕАЛИЗАЦИИ УГРОЗЫ:

- получение доступа к информации, составляющей коммерческую тайну;
- склонение к саботажу в интересах конкурента

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗЫ СКЛОНЕНИЯ СОТРУДНИКОВ К НАРУШЕНИЮ ОБЯЗАТЕЛЬСТВ ПЕРЕД РАБОТОДАТЕЛЕМ СО СТОРОНЫ КОНКУРЕНТОВ ЕГО КЛИЕНТОВ

ОБЪЕКТ УГРОЗЫ:

сотрудники организации, имеющие доступ к конфиденциальной клиентской информации

ЦЕЛИ РЕАЛИЗАЦИИ УГРОЗЫ: получение доступа к информации, составляющей клиентскую тайну

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗЫ СКЛОНЕНИЯ СОТРУДНИКОВ К НАРУШЕНИЮ ОБЯЗАТЕЛЬСТВ ПЕРЕД РАБОТОДАТЕЛЕМ СО СТОРОНЫ КРИМИНАЛЬНЫХ ГРУППИРОВОК И ИНДИВИДУАЛЬНЫХ ЗЛОУМЫШЛЕННИКОВ

ОБЪЕКТ УГРОЗЫ:

- сотрудники финансовой службы
- сотрудники, отвечающие за хранение ликвидных товарно-материальных ценностей
- специалисты, отвечающие за систему электронных платежей и расчетов

ЦЕЛИ РЕАЛИЗАЦИИ УГРОЗЫ:

- проверка правильности исчисления выплат рэкетирской группировке («крыше»);
- склонение к соучастию в хищениях денежных средств;
- склонение к соучастию в хищении товарно-материальных ценностей;
- получение электронных кодов доступа

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗЫ СКЛОНЕНИЯ СОТРУДНИКОВ К НАРУШЕНИЮ ОБЯЗАТЕЛЬСТВ ПЕРЕД РАБОТОДАТЕЛЕМ СО СТОРОНЫ НАЛОГОВЫХ И ДРУГИХ ГОСУДАРСТВЕННЫХ ОРГАНОВ

ОБЪЕКТ УГРОЗЫ:

- сотрудники финансовой службы;
- сотрудники службы информационных технологий

ЦЕЛИ РЕАЛИЗАЦИИ УГРОЗЫ:

- проверка правильности исчисления налоговых выплат;
- проверка легитимности бизнеса и отсутствия связей с криминалитетом и террористическими группировками

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗЫ СКЛОНЕНИЯ СОТРУДНИКОВ К НАРУШЕНИЮ СВОИХ ОБЯЗАТЕЛЬСТВ ПЕРЕД РАБОТОДАТЕЛЕМ СО СТОРОНЫ ИНОСТРАННЫХ СПЕЦСЛУЖБ

ОБЪЕКТ УГРОЗЫ:

сотрудники организации, имеющие доступ к секретной информации о деятельности государства, организаций ВПК

ЦЕЛЬ РЕАЛИЗАЦИИ УГРОЗЫ:

получение доступа к информации, составляющей государственную или военную тайну

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗЫ СКЛОНЕНИЯ СОТРУДНИКОВ К НАРУШЕНИЮ ОБЯЗАТЕЛЬСТВ ПЕРЕД РАБОТОДАТЕЛЕМ СО СТОРОНЫ ДРУГИХ СОТРУДНИКОВ ОРГАНИЗАЦИИ

ОБЪЕКТ УГРОЗЫ:

- непосредственные подчиненные;
- коллеги по работе;
- сотрудники других подразделений

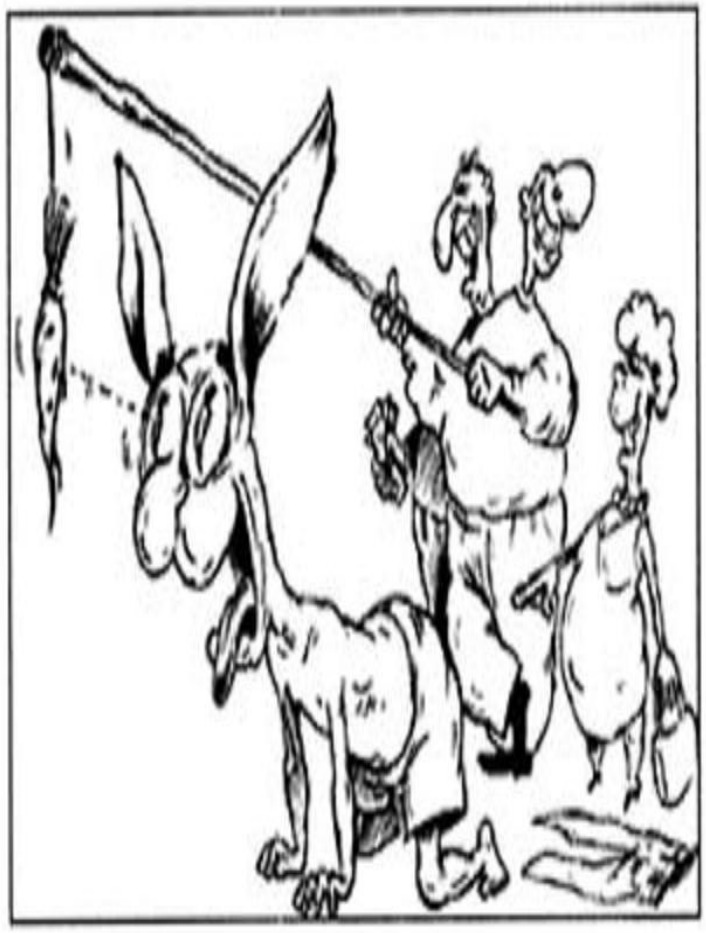
ЦЕЛИ РЕАЛИЗАЦИИ УГРОЗЫ:

- склонение к соучастию в любых должностных преступлениях;
- вербовка от имени сторонней организации;
- сокрытие от работодателя компрометирующей информации

МЕТОДЫ ПРОФИЛАКТИКИ УГРОЗЫ:

- организация тщательного отбора кандидатов на трудоустройство в целях заблаговременного отсева лиц, чьи личностные качества или автобиографические данные делают их особенно уязвимыми для вербовки или шантажа;
- обучение сотрудников правилам служебного и внеслужебного поведения, исключающего возможность их последующего шантажа;
- специальное обучение сотрудников правилам поведения в случае попыток их вербовки, шантажа, или декларации угроз;
- постоянный контроль над сотрудниками, занимающими рабочие места, наиболее опасные с позиции рассматриваемой угрозы (имущественное положение, образ жизни, новые привычки, стиль поведения, психологическое состояние и т.п.);
- специальные служебные проверки сотрудников, в отношение которых у руководителя или службы безопасности по результатам оперативного контроля появились обоснованные подозрения.

ЛИЧНОСТНЫЕ КАЧЕСТВА КАНДИДАТА НА ТРУДОУСТРОЙСТВО, НАЛИЧИЕ КОТОРЫХ ПОВЫШАЕТ ВЕРОЯТНОСТЬ УСПЕШНОГО СКЛОНЕНИЯ ЕГО К НАРУШЕНИЮ ОБЯЗАТЕЛЬСТВ ПЕРЕД РАБОТОДАТЕЛЕМ



- **повышенный меркантилизм (жадность к деньгам);**
- излишняя амбициозность;
- повышенная коммуникабельность;
- завышенная самооценка (комплекс «личного превосходства»);
- заниженная самооценка (комплекс «собственной неполноценности»);
- эгоизм;
- трусливость;
- завистливость;
- повышенная внушаемость;
- неспособность к самоконтролю;
- неуважение к окружающим;
- психическая неуравновешенность;
- обидчивость и злопамятность

ДРУГИЕ ЛИЧНОСТНЫЕ КАЧЕСТВА КАНДИДАТА НА ТРУДОУСТРОЙСТВО, НАЛИЧИЕ КОТОРЫХ ПОВЫШАЕТ ВЕРОЯТНОСТЬ УСПЕШНОГО СКЛОНЕНИЯ ЕГО К НАРУШЕНИЮ ОБЯЗАТЕЛЬСТВ ПЕРЕД РАБОТОДАТЕЛЕМ

ПРИВЫЧКИ:

- наркологическая или алкогольная зависимость;
- склонность к азартным играм;
- дорогостоящие увлечения (коллекционирование, высоко затратные виды отдыха и пр.);
- неразборчивость в личных связях

АВТОБИОГРАФИЧЕСКИЕ ДАННЫЕ:

- криминальное прошлое;
- нарушенные финансовые обязательства перед прежним работодателем или финансовыми учреждениями;
- повышенная мобильность на рынке труда в форме регулярной смены работодателей;
- сомнительные, с позиции интересов обеспечения безопасности работодателя, родственные связи и знакомства;
- хронические заболевания, требующие дорогостоящего лечения

МЕТОДЫ ПРЕСЕЧЕНИЯ УГРОЗЫ И НАКАЗАНИЯ ВИНОВНИКА:

- перевод сотрудника, чья потенциальная лояльность работодателю вызывает обоснованные сомнения, на другое рабочее место, объективно неинтересное для потенциальных субъектов угрозы;
- мотивация сотрудника, своевременно проинформировавшего службу безопасности о попытке его вербовки или угроз в его адрес;
- освобождение сотрудника от ответственности за уже допущенные нарушения, ставшие поводом для шантажа, в случае своевременного информирования службы безопасности об этой попытке (при тяжелых нарушениях такой сотрудник, несет ответственность в минимально возможном объеме);
- увольнение сотрудника, ставшего «агентом влияния» субъекта рассматриваемой угрозы, в случае подтверждения его вины;
- использование завербованного сотрудника в качестве источника дезинформации, с последующим его увольнением;
- использование предусмотренных законом методов уголовного преследования виновных сотрудников.

ПРИЧИНЫ РЕАЛИЗАЦИИ УГРОЗЫ:

- участие в борьбе за раздел или последующий передел государственной собственности (например, за контрольный пакет акций нефтяной компании, горно-обогатительного комбината, крупного отеля), осуществляемой с использованием нелегитимных методов;
- конфликты, связанные с рейдерским захватом чужого бизнеса;
- конфликты между конкурентами (физическая ликвидация конкурента как «последний довод» в конкурентной борьбе);
- невыполнение обязательств, принятых на себя в рамках прямого сотрудничества жертвы покушения с «теневой» экономикой и организованной преступностью («отмывание» денег и перевод их за рубеж, операции с «черным налом», выделение квот, содействие в недружественном поглощении чужого бизнеса, разглашение информации);
- невыполнение принятых на себя обязательств в отношении крупных клиентов и партнеров;
- борьба за контроль над конкретной организацией между двумя преступными группировками, если ее высшее руководство занимает сторону одной из них;
- нерешенные внутрикорпоративные проблемы (например, конфликты между совладельцами бизнеса или топ-менеджерами).

СУБЪЕКТЫ УГРОЗЫ:

а). Внешние:

- конкуренты;
- криминальные структуры.

б). Внутренние:

- совладелец бизнеса;
- один из топ-менеджеров, близких по должностному статусу.

ОБЪЕКТЫ УГРОЗЫ:

- собственники организации;
- топ менеджеры организации или высокопоставленные государственные служащие;
- особо доверенные сотрудники – «секретоносители».

МЕТОДЫ РЕАЛИЗАЦИИ УГРОЗЫ

- открытое покушение, реализуемое с помощью традиционных методов и автоматически вызывающее возбуждение по факту покушения уголовного дела;
- имитация самоубийства объекта покушения;
- скрытое покушение с использованием нетрадиционных средств (специальные химические препараты из арсенала спецслужб, радиоактивные изотопы и т.п.), имитирующие смерть объекта угрозы от естественных причин.

МЕТОДЫ ПРОФИЛАКТИКИ УГРОЗЫ:

- принципиальный отказ от работы в сфере бизнеса или участия в конкретных операциях, где рассматриваемая угроза становится реальной;
- строгое соблюдение правил и норм, неформально сложившихся в соответствующей сфере бизнеса;
- эффективная деловая разведка и контрразведка, направленная на заблаговременное выявление потенциально опасных ситуаций;
- решение проблемы путем ликвидации самой причины готовящегося покушения (урегулирование конфликтной ситуации в процессе переговоров, реализация принятых обязательств и т.п.);
- специальное обучение собственников и топ-менеджеров организации правилам обеспечения собственной физической безопасности.

МЕТОДЫ ПРЕСЕЧЕНИЯ УГРОЗЫ:

- **решение проблемы путем использования угроз адекватного воздействия на самого заказчика;**
- **усиление защиты объекта покушения до уровня, делающего угрозу практически нереализуемой;**
- **обращение за помощью к правоохранительным органам (наименее эффективное решение, целесообразное лишь для организаций, реализующих стратегию «пассивной защиты»).**

ПРАВИЛА ПОДБОРА ЛИЧНЫХ ТЕЛОХРАНИТЕЛЕЙ И РАБОТЫ С НИМИ:

- при комплектации службы штатными сотрудниками предпочтение следует отдавать профессиональным телохранителям, получившим специальную подготовку в государственных или частных структурах;
- использовать телохранителей, «замаскированных» под секретарей, помощников, пресс-атташе или просто случайных прохожих, чьи внешние данные принципиально не совпадают с имиджем «бодигарда» (например, хрупкая девушка, пожилой мужчина, субтильный интеллигент);
- в составе службы целесообразно выделять контингент постоянных личных телохранителей ограниченного числа высших руководителей и дежурных телохранителей для разовой охраны других специалистов (например, на время их служебной командировки)

Задание

Сформулируйте основные причины реализации угрозы успешного переманивания наиболее ценных сотрудников организации.

Домашнее задание

Определите, какие личностные качества делают сотрудника особенно уязвимым в отношении угрозы склонения его к нарушению доверия со стороны работодателя.

Литература

1. Алавердов А.Р. Управление кадровой безопасностью организации: учебник. – М.: Маркет ДС, 2008. – 176 с. – (Университетская серия).
2. Соломанидин В.Г., Соломанидина Т.О. Кадровая безопасность компании. – М.: Альфа-Пресс, 2011. – 688с.

Тема 4.

Противодействие угрозам информационной безопасности организации со стороны собственного персонала

УЧЕБНЫЕ ВОПРОСЫ ТЕМЫ

4.1 Конфиденциальная информация как объект защиты

4.2 Типовые причины, формы и методы реализации угроз информационной безопасности организации с участием ее персонала

4.3 Методы противодействия угрозам информационной безопасности организации со стороны ее персонала

4.4 Управление персоналом организации в целях обеспечения ее информационной безопасности

КЛАССИФИКАЦИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ КАК ОБЪЕКТА ЗАЩИТЫ

ПО ПРИЗНАКУ ЕЕ ХАРАКТЕРА:

- ***политическая информация,*** например, отсутствующие в открытых источниках сведения об ожидаемых изменениях политической ситуации, законодательства, других политических факторах, способных повлиять на рыночное положение организации или ее контрагентов;
- ***экономическая информация,*** например, отсутствующие в открытых источниках сведения об экономической ситуации в конкретных регионах и отраслях;
- ***финансовая информация,*** например, отсутствующие в открытых источниках сведения о финансовом состоянии клиентов и других партнерах банка;
- ***коммерческая информация,*** например, результаты проведенного специалистами организации анализа соответствующих рынков или его планы их освоения;
- ***технологическая информация,*** например, сведения об уже разработанных, но еще не внедренных организацией новых технологий;
- ***управленческая информация,*** например, сведения об используемых организацией методах управления по конкретным направлениям собственной деятельности.

КЛАССИФИКАЦИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ КАК ОБЪЕКТА ЗАЩИТЫ

ПО ПРИЗНАКУ ЕЕ СОДЕРЖАНИЯ:

- информация, содержащая клиентскую тайну;
- информация, содержащая коммерческую тайну, т.е. сведения, разглашение которых способно нанести ущерб интересам самой организации.

ПО ПРИЗНАКУ ИСПОЛЬЗУЕМОГО НОСИТЕЛЯ:

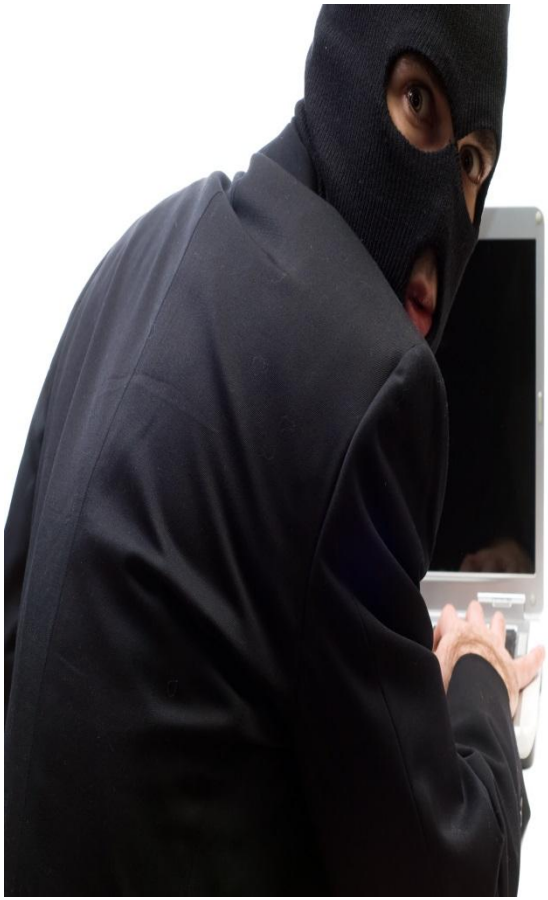
- информацию в устном виде, например, сведения, обсуждаемые в процессе делового совещания;
- информацию на бумажных носителях, т.е. традиционная форма документов, используемых организацией;
- информацию в электронном виде, т.е. компьютерные базы данных, а также сведения, передаваемые по компьютерным коммуникациям или телефонным сетям (приоритетный объект защиты в современных условиях).

КЛАССИФИКАЦИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ КАК ОБЪЕКТА ЗАЩИТЫ

ПО ПРИЗНАКУ СТЕПЕНИ КОНФЕДЕНЦИАЛЬНОСТИ:

- ***абсолютно конфиденциальная,*** содержащая секретные сведения, разглашение которых способно нанести ущерб стратегического характера;
- ***строго конфиденциальная,*** содержащая особо секретные сведения;
- ***конфиденциальная,*** содержащая секретные сведения;
- ***для служебного пользования,*** содержащая наименее секретные сведения, не предназначенные лишь для открытой печати.

ТИПОВЫЕ ФОРМЫ РЕАЛИЗАЦИИ УГРОЗ информационной безопасности:



- ***перехват конфиденциальной информации,*** в результате которого у субъекта угрозы оказывается ее дубликат (особая опасность этой формы угрозы для пострадавшей организации заключается в том, что о самом факте утечки она, чаще всего, узнает лишь после того, когда конечная цель перехвата уже достигнута);
- ***хищение конфиденциальной информации,*** в результате которого субъект угрозы одновременно решает две задачи – приобретает соответствующие сведения и лишает их пострадавшую организацию;
- ***повреждение или уничтожение конфиденциальной информации,*** в результате которого субъектом угрозы достигается лишь задача нанесения ущерба атакуемой организации;
- ***искажение конфиденциальной информации,*** в результате которого атакованная организация может принять изначально ошибочное управленческое решение или оказаться скомпрометированной в глазах контрагентов или государства.

ПЕРЕЧЕНЬ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ

- несанкционированное проникновение в защищенные базы данных с использованием специальных хакерских программ с целью последующего копирования или искажения накопленных сведений;
- копирование или искажение электронных баз данных, к которым у нелояльного сотрудника имеется санкционированный доступ;
- передача третьему лицу паролей и кодов доступа к конфиденциальным электронным базам данных;
- повреждение или уничтожение электронных баз данных с использованием компьютерных вирусов;
- подключение к компьютерам организации специальных электронных устройств или использование специальных программ (типа «Троянский конь»), позволяющих копировать и передавать по электронной почте соответствующие данные;
- нарушение правил работы с конфиденциальной информацией в электронной форме, позволяющее заинтересованным лицам (нелояльным коллегам по работе, посетителям офиса организации и т. п.) получить к ней несанкционированный доступ

ПЕРЕЧЕНЬ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА БУМАЖНЫХ НОСИТЕЛЯХ

- копирование документов;
- хищение документов;
- искажение документов;
- уничтожение документов;
- нарушение правил работы с конфиденциальными документами, позволяющее заинтересованным лицам получить к ним несанкционированный доступ

ПЕРЕЧЕНЬ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В УСТНОЙ ФОРМЕ

- подслушивание информации без использования технических средств;
- выведование информации у коллег по работе;
- установка стационарных или временных подслушивающих устройств;
- устное разглашение доверенной информации в силу злого умысла;
- отключение технических средств защиты устной информации от подслушивания (со злым умыслом или в силу простой безответственности);
- нарушение правил работы с конфиденциальной информацией в устной форме, позволяющее заинтересованным лицам получить к ней несанкционированный доступ

ТИПОВЫЕ ПРИЧИНЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ ПО ВИНЕ БЕЗОТВЕТСТВЕННЫХ СОТРУДНИКОВ

- запись паролей и кодов доступа в настольном календаре, на задней части монитора или нижней панели клавиатуры компьютера;
- игнорирование требования о выходе из «закрытого» каталога или отключении компьютера при необходимости покинуть рабочее место даже на несколько минут;
- использование собственных дискет или CD дисков с переносом информации из них в рабочий компьютер (угроза занесения вируса);
- разрешение клиенту или другому постороннему лицу воспользоваться компьютером, содержащим закрытую информацию;
- передача конфиденциальных данных по электронной почте на домашний адрес или копирование на собственный носитель (флешку, CD диск) с последующим их выносом из здания организации для работы в домашних условиях.

ТИПОВЫЕ ПРИЧИНЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА БУМАЖНЫХ НОСИТЕЛЯХ ПО ВИНЕ БЕЗОТВЕТСТВЕННЫХ СОТРУДНИКОВ

- игнорирование требования о перемещении конфиденциальных документов в сейф, шкаф или закрывающийся на замок ящик при необходимости покинуть рабочее место;
- запись шифра замка сейфа в записной книжке, настольном календаре и т.п., а также хранение ключей в доступном для посторонних месте;
- вынос конфиденциальных документов из здания организации для работы с ними в домашних условиях.

ТИПОВЫЕ ПРИЧИНЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В УСТНОЙ ФОРМЕ ПО ВИНЕ БЕЗОТВЕТСТВЕННЫХ СОТРУДНИКОВ

334. Иванов К., Брискин В.
Болтовня, сплетни — на руку врагу. 1954

- **игнорирование требования о проведении конфиденциальных переговоров только в специально предназначенных для этого помещениях;**
- **обсуждение конфиденциальной информации с не допущенными к ней лицами (коллегами по работе, родственниками, друзьями);**
- **нарушение работоспособности технических средств, обеспечивающих защиту устной информации (например, не включение генератора помех в защищенном от прослушивания помещении);**
- **использование не защищенных каналов связи в процессе телефонных переговоров.**

ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ПЕРВЫЙ ЭТАП: Ранжирование конфиденциальной информации как объекта защиты»

Информация с грифом «АБСОЛЮТНО КОНФИДЕНЦИАЛЬНО»:

- информация, составляющая клиентскую тайну, разглашение которой способно нанести стратегический ущерб интересам клиентов или подконтрольным организациям);
- закрытая информация о собственниках организации;
- информация о стратегических планах организации по коммерческому и финансовому направлениям деятельности;
- любая информация о деятельности службы безопасности, реализуемой в рамках стратегий «упреждающего противодействия» и, частично, «адекватного ответа»;
- прикладные методы защиты информации, используемые организацией (коды, пароли, программы).

ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ПЕРВЫЙ ЭТАП: Ранжирование конфиденциальной информации как объекта защиты»

Информация с грифом «СТРОГО КОНФИДЕНЦИАЛЬНО»:

- все прочие конфиденциальные сведения о клиентах;
- информация маркетингового, финансового и технологического характера, составляющая коммерческую тайну;
- информация о сотрудниках организации, содержащуюся в индивидуальных досье.

ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ПЕРВЫЙ ЭТАП: Ранжирование конфиденциальной информации как объекта защиты»

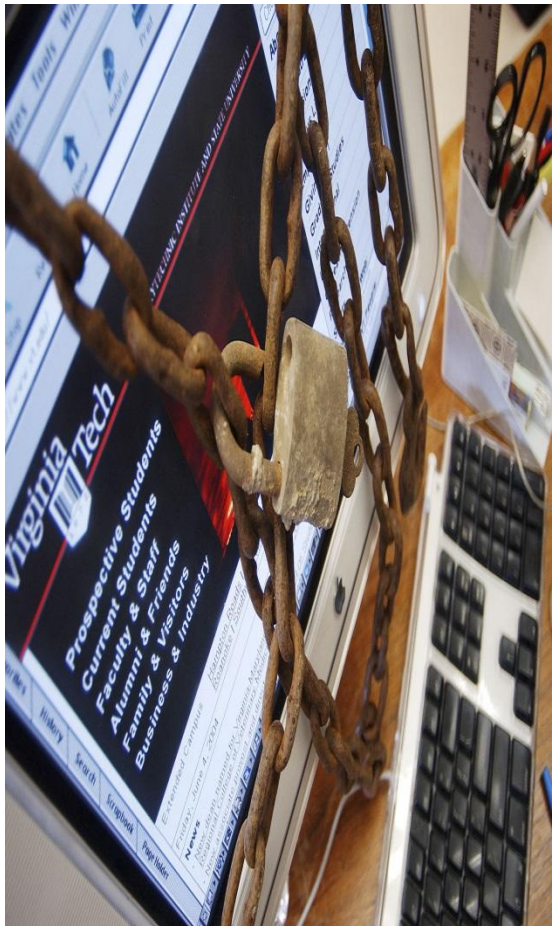
Информация с грифом «КОНФИДЕНЦИАЛЬНО»:

- базы данных по направлениям деятельности организации, созданные и поддерживаемые в качестве элементов обеспечения соответствующих систем управления;
- сведения о заработной плате и индивидуальных «социальных пакетах» сотрудников организации, а также составе «резерва на выдвижение»;
- внутренние регламенты (положения, инструкции, приказы и т.п.) используемые в системе внутрикорпоративного менеджмента;
- внутренние регламенты (положения, инструкции, приказы и т.п.) используемые в системе внутрикорпоративного менеджмента.

Информация с грифом «ДСП»: вся прочая информация, не предназначенная для публикаций в открытой печати

ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ВТОРОЙ ЭТАП: Определение перечня прикладных методов защиты информации



МЕТОДЫ ПРОГРАММНО-МАТЕМАТИЧЕСКОГО ХАРАКТЕРА:

- программы, ограничивающие доступ в компьютерные сети и отдельные компьютеры организации;
- программы, защищающие информацию от повреждения умышленно или случайно занесенными вирусами (автоматическое тестирование при включении компьютера, при использовании СД - дисков или дискет);
- программы, автоматически кодирующие (шифрующие) информацию;
- программы, препятствующие перезаписи информации, находящейся в памяти компьютера, на внешние носители или через сеть;
- программы, автоматически стирающие определенные данные с ограниченным для конкретного пользователя временем доступа.

ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ВТОРОЙ ЭТАП: Определение перечня прикладных методов защиты информации

МЕТОДЫ ТЕХНИЧЕСКОГО ХАРАКТЕРА:

- использование экранированных помещений для проведения конфиденциальных переговоров;
- использование специальных хранилищ и сейфов для хранения информации на бумажных носителях (при необходимости с устройствами автоматического уничтожения ее при попытке несанкционированного проникновения);
- использование детекторов и иной аппаратуры для выявления устройств перехвата информации;
- использование защищенных каналов телефонной связи;
- использование средств подавления работы устройств перехвата информации;
- использование средств автоматического кодирования (шифровки) устной и письменной информации.

ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ВТОРОЙ ЭТАП: Определение перечня прикладных методов защиты информации

МЕТОДЫ ОРГАНИЗАЦИОННОГО ХАРАКТЕРА:

- мероприятия по ограничению доступа к конфиденциальной информации (общережимные мероприятия, системы индивидуальных допусков, запрет на вынос документов из соответствующих помещений, возможность работы с соответствующей компьютерной информацией лишь с определенных терминалов и т.п.);
- мероприятия по снижению возможности случайного или умышленного разглашения информации или других форм ее утечки (правила работы с конфиденциальными документами и закрытыми базами данных, проведения переговоров, поведения сотрудников организации на службе и вне ее);
- мероприятия по дроблению конфиденциальной информации, не позволяющие сосредоточить в одном источнике (у сотрудника, в документе, файле и т.п.) все сведения по вопросу, интересующему потенциального субъекта угроз;
- мероприятия по контролю над соблюдением установленных правил информационной безопасности;
- мероприятия при выявлении фактов утечки той или иной конфиденциальной информации.

ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ТРЕТИЙ ЭТАП: Разработка и внедрение системы управления информационной безопасностью

ОСНОВНЫЕ ПОЛОЖЕНИЯ КОНЦЕПЦИИ УПРАВЛЕНИЯ:

- принципы ранжирования конфиденциальной информации по степени ее важности для организации, следовательно, по требованиям к эффективности защиты;
- подходы к обеспечению системы программными продуктами (самостоятельная разработка или заказ на стороне);
- подходы к распределению ответственности за обеспечение информационной безопасности между уполномоченными штабными службами организациями (безопасности, персонала, маркетинга, информационных технологий) и производственными подразделениями;
- подходы к выбору методов пресечения выявленных угроз;
- подходы к выделению ресурсов, необходимых для профилактики и пресечения возможных угроз (фиксированный процент от общей суммы собственных расходов организации, выделение средств под представленные сметы и целевые программы и т.п.);
- критерии оценки эффективности защиты конфиденциальной информации

ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ТРЕТИЙ ЭТАП: Разработка и внедрение системы управления информационной безопасностью

СОСТАВ ВНУТРЕННЕЙ НОРМАТИВНОЙ БАЗЫ:

- общие для всей организации регламенты (например, «Положение о правилах обеспечения информационной безопасности», «Правила проведения конфиденциальных переговоров», «Правила работы с закрытыми базами данных», «Перечень сведений, составляющих коммерческую и клиентскую тайну» и т.п.),
- внутренние регламенты службы безопасности, включая должностные инструкции ее сотрудников, специализирующихся в этой области;
- правила обеспечения информационной безопасности, фиксируемых в регламентах конкретных структурных подразделений и должностных инструкциях их сотрудников

ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ТРЕТИЙ ЭТАП: Разработка и внедрение системы управления информационной безопасностью

РАСЧЕТ И ВЫДЕЛЕНИЕ ФИНАНСОВЫХ РЕСУРСОВ

необходимых:

- для приобретения (самостоятельной разработки), эксплуатации и обновления программных средств и средств инженерно-технической защиты;
- для проведения соответствующих организационных мероприятий;
- службе безопасности для осуществления специальных профилактических и контрольных мероприятий

ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

ТРЕТИЙ ЭТАП: Разработка и внедрение системы управления информационной безопасностью

ОБУЧЕНИЕ ПЕРСОНАЛА:

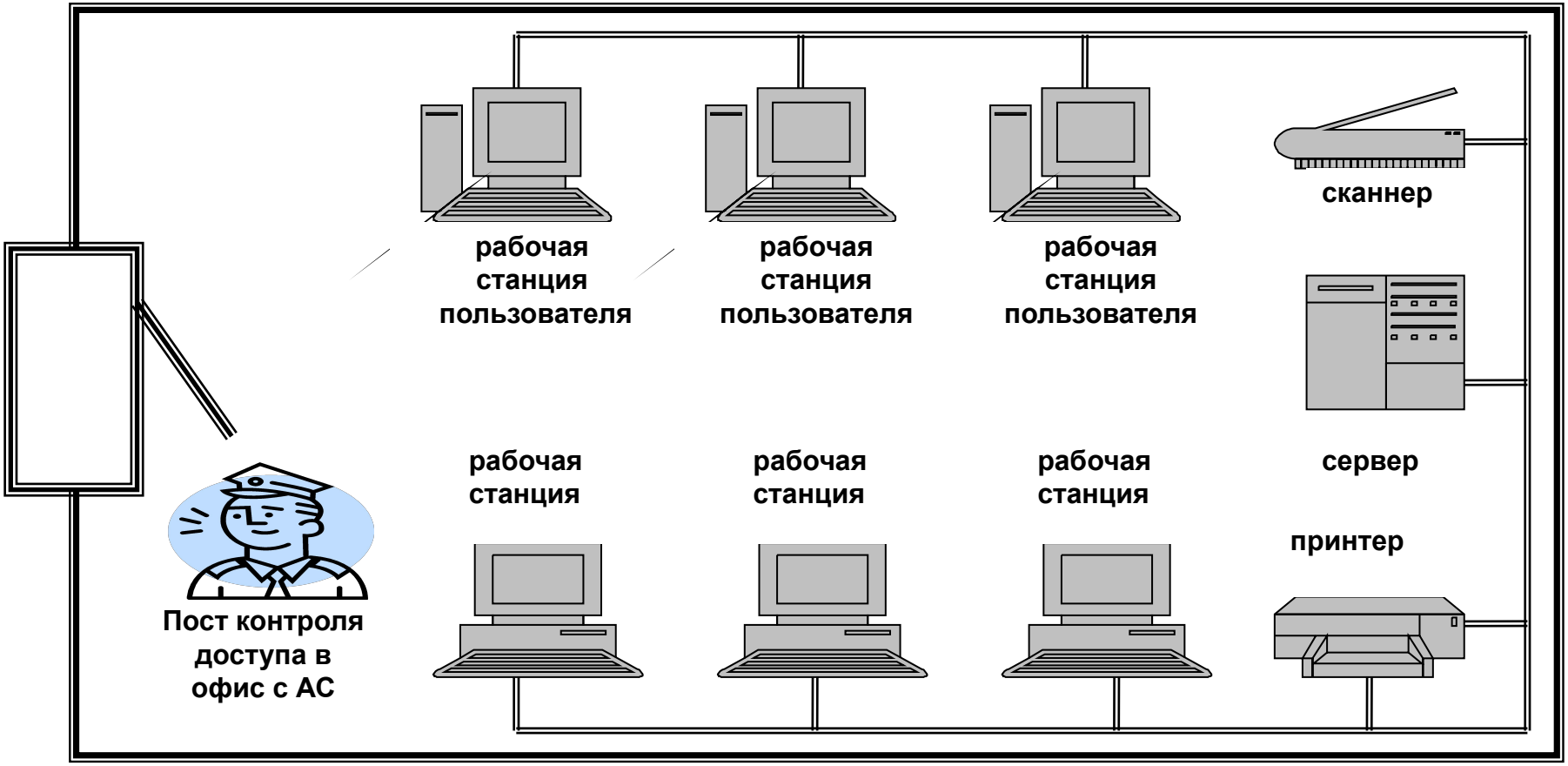
- сотрудников самой службы безопасности;
- новых сотрудников организации в режиме первичного обучения;
- прочих сотрудников организации в режиме повышения квалификации

ОЦЕНКА ЭФФЕКТИВНОСТИ:

- функционирования системы в целом;
- соответствующего направления работы службы безопасности;
- соответствующего направления работы руководителей структурных подразделений организации

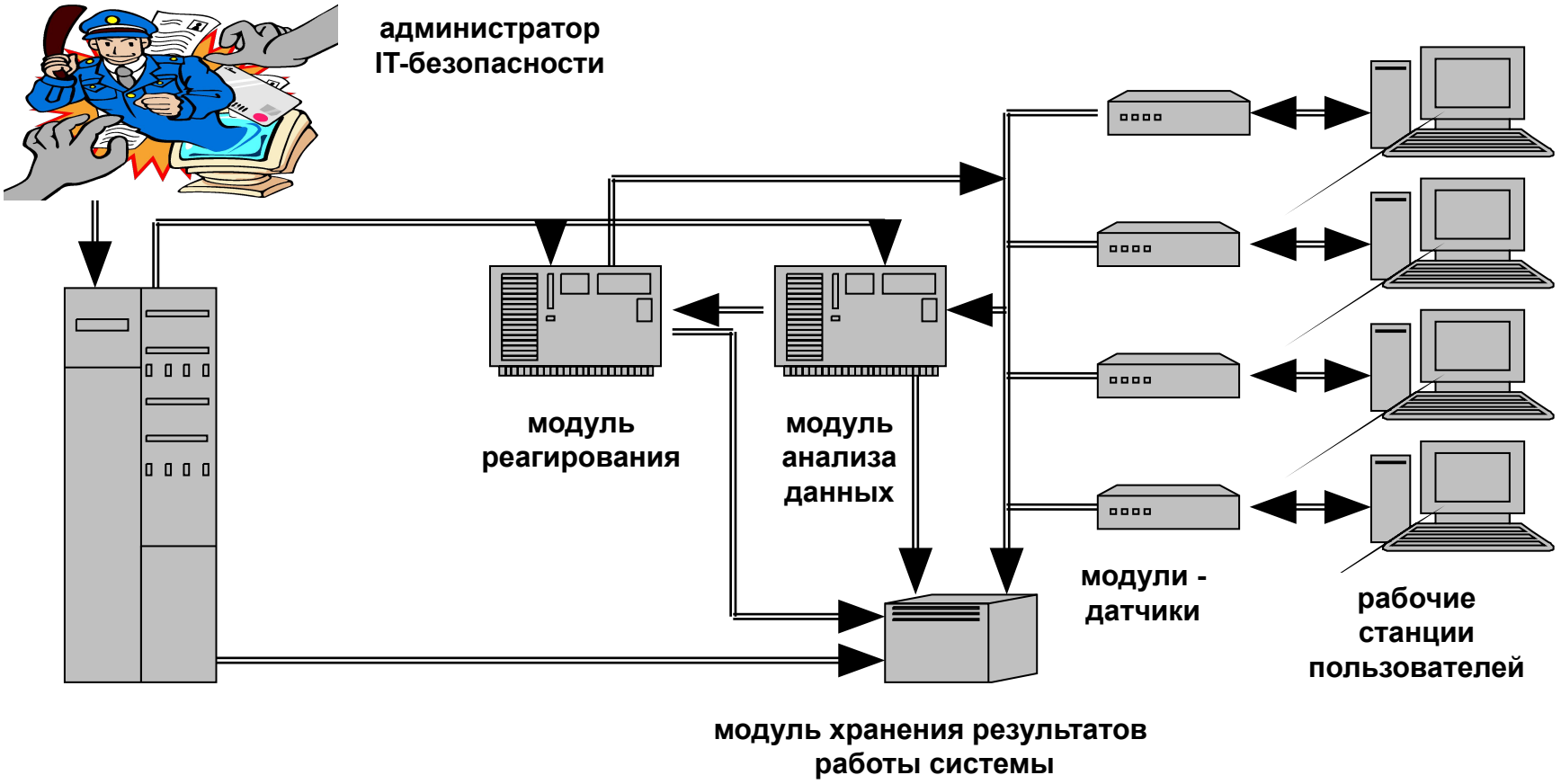
ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Методы защиты информации в электронной форме: защищенный офис



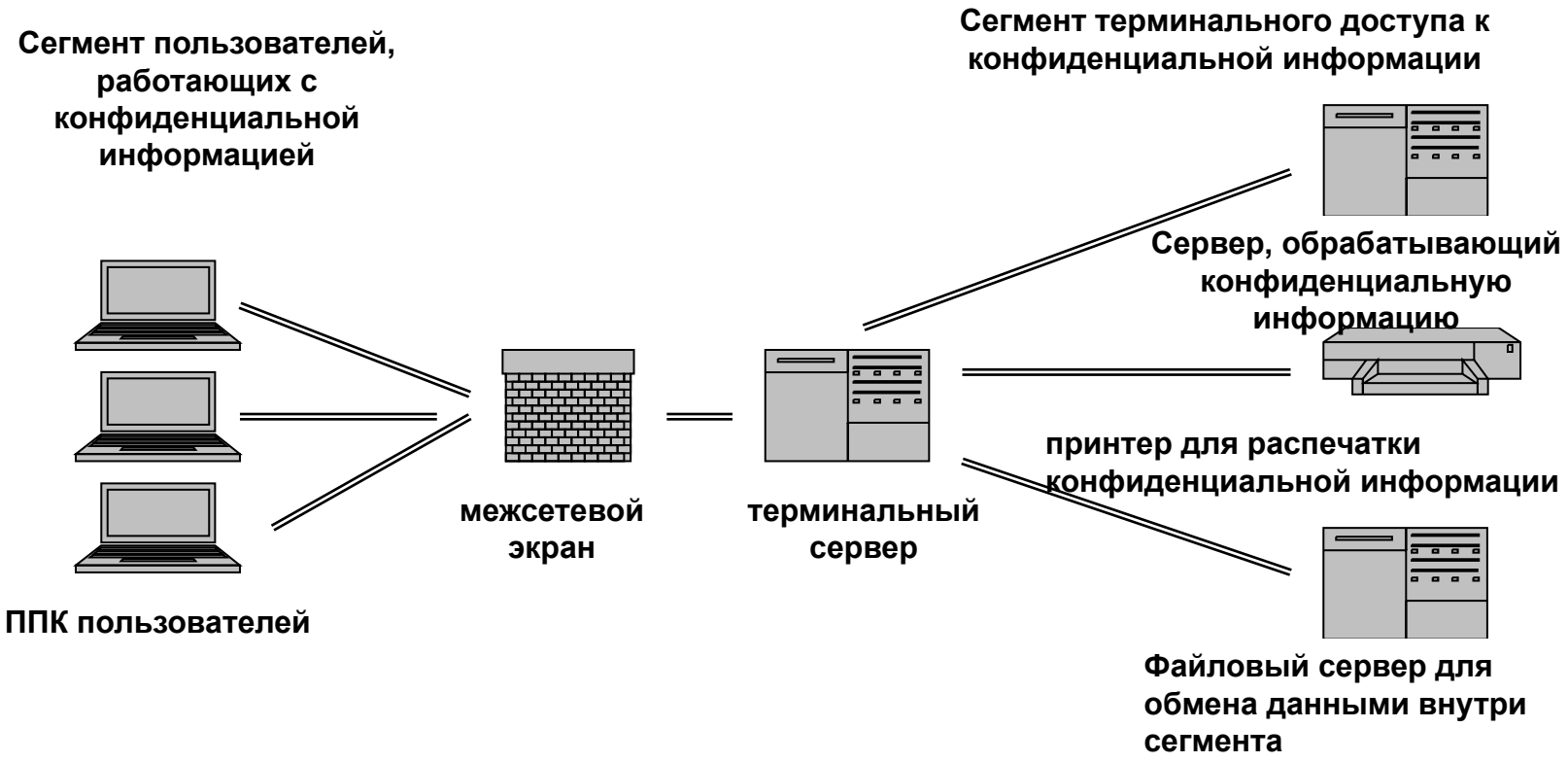
ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Методы защиты информации в электронной форме: защищенная локальная сеть



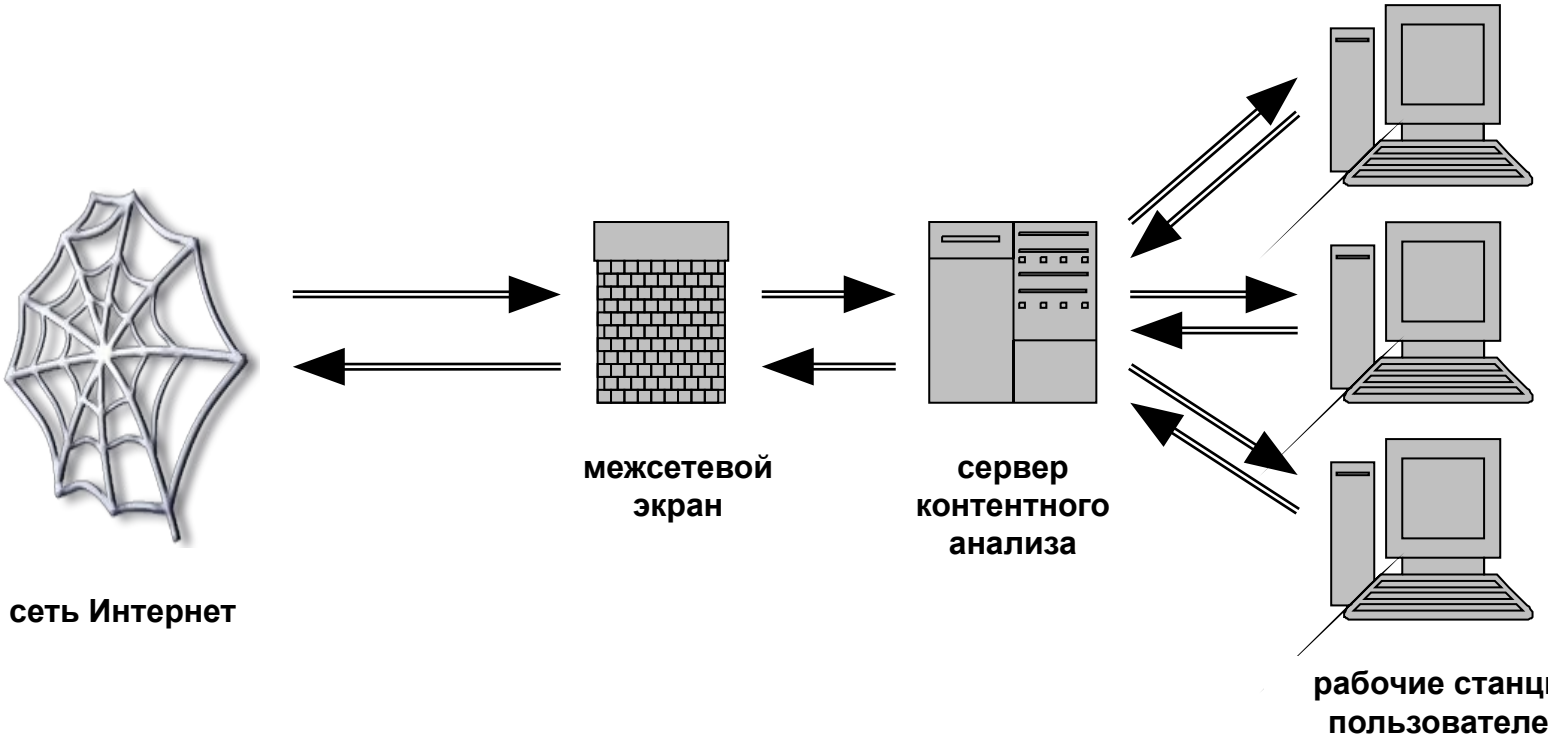
ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Методы защиты информации в электронной форме: защищенный сегмент пользователей



ТЕХНОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Методы защиты информации в электронной форме: защита от нежелательных контактов через Интернет



ОБЩИЕ МЕТОДИЧЕСКИЕ ТРЕБОВАНИЯ к организации специальной подготовки персонала:

- распространение подготовки на все категории персонала организации, с дифференциацией ее форм и методов по должностным категориям обучаемых;
- непрерывность подготовки, что обеспечивается регулярным проведением специальных профилактических бесед или разбором уже состоявшихся угроз в адрес организации;
- привлечение к подготовке не только специалистов службы безопасности, но и руководителей структурных подразделений, обычно имеющих в глазах своих подчиненных больший авторитет;
- использование в процессе обучения наряду с теоретическими материалами практических примеров из деятельности своей и сторонних организаций;
- использование методов обучения, способных вызвать интерес обучаемых к самому процессу подготовки, например, ролевые игры, видеозаписи, демонстрация некоторых технических средств защиты и т.п.

ФОРМЫ СПЕЦИАЛЬНОЙ ПОДГОТОВКИ ПЕРСОНАЛА

ПЕРВИЧНАЯ ПОДГОТОВКА:

- инструктаж со стороны специалиста службы безопасности;
- инструктаж со стороны непосредственного руководителя или персонального куратора (наставника).

ФОРМЫ СПЕЦИАЛЬНОЙ ПОДГОТОВКИ ПЕРСОНАЛА

ПОСЛЕДУЮЩАЯ ПОДГОТОВКА осуществляется службой безопасности дифференцированно по категориям сотрудников организации:

- ***для высшего руководства*** – в форме специальных аналитических обзоров, ежемесячно представляемых им за подписью вице-президента по безопасности;
- ***для руководителей структурных подразделений*** – в форме ежеквартальных встреч с вице-президентом по безопасности;
- ***для остального персонала*** - в форме специального инструктажа, который не реже одного раза в квартал проводится одним из специалистов службы безопасности непосредственно в структурных подразделениях.

КОНТРОЛЬ НАД СОТРУДНИКАМИ ОРГАНИЗАЦИИ

СУБЪЕКТЫ КОНТРОЛЯ:

- служба безопасности;
- руководители структурных подразделений.

ОБЪЕКТЫ КОНТРОЛЯ:

- исполнение сотрудниками установленных правил обеспечения информационной безопасности работодателя;
- лояльность сотрудников.

КОНТРОЛЬ НАД СОТРУДНИКАМИ ОРГАНИЗАЦИИ

Профилактический контроль над соблюдением правил обеспечения безопасности проводится с использованием следующих методов:

- плановых и внезапных проверок, в процессе которых служба безопасности проверяет соблюдения в структурных подразделениях правил работы с конфиденциальной информацией, а также работоспособность технических средств защиты;
- мониторинга ситуации с использованием специальных технических средств наблюдения;
- мониторинга ситуации силами нештатных информаторов службы безопасности из числа сотрудников соответствующих подразделений.

Контроль личной лояльности персонала осуществляется службой безопасности в отношении сотрудников:

- занимающих ключевые рабочие места, обеспечивающие доступ к особо конфиденциальной информации;
- привлекших внимание службы безопасности своим поведением или иными фактами, ставящими под сомнение их потенциальную лояльность

КОНТРОЛЬ НАД СОТРУДНИКАМИ ОРГАНИЗАЦИИ

Факты, ставящие под сомнение потенциальную лояльность сотрудника работодателю:

- необъяснимое объективными причинами внезапное улучшение материального положения сотрудника или контактирующих с ним родственников;
- не вызванные служебной необходимостью контакты с представителями субъектов потенциальных угроз (конкурентов, криминальных структур и т.п.);
- изменение образа жизни сотрудника или появление привычек и личностных качеств, делающих его уязвимым для вербовки и шантажа;
- зафиксированные регулярные высказывания недовольства работодателем, служебным положением, доходами и т.п.

МОТИВАЦИЯ СОТРУДНИКОВ ОРГАНИЗАЦИИ

ПЕРЕЧЕНЬ СПЕЦИАЛЬНЫХ ПООЩРЕНИЙ:

- сотрудников службы информационных технологий и других подразделений, разработавших новые программные средства, повышающие степень защищенности компьютерных баз данных и коммуникаций;
- сотрудников службы безопасности, выявивших источники утечки конфиденциальной информации, разработавших новые технологии или методы защиты информации в устной форме и на бумажных носителях, успешно завершивших особо важные оперативные мероприятия по отражению реализуемых угроз информационной безопасности;
- руководителей структурных подразделений, к сотрудникам которых у службы безопасности в течение отчетного года не было ни одного замечания в части соблюдения правил обеспечения информационной безопасности;
- любых сотрудников организации, оказавшим службе безопасности реальную помощь в выявлении источников угроз информационной безопасности

САНКЦИИ К СОТРУДНИКАМ ОРГАНИЗАЦИИ

ПЕРЕЧЕНЬ АДМИНИСТРАИВНЫХ САНКЦИЙ:

- увольнение сотрудника за невыполнение принятых на себя трудовых обязательств в форме однократного грубого или неоднократных мелких нарушений правил обеспечения информационной безопасности;
- отказ в пролонгации трудового договора;
- досрочное прекращение действия трудового договора в связи с неудовлетворительными результатами прохождения испытательного срока;
- перевод сотрудника на другое рабочее место (в том числе - в другом подразделении), не предполагающее доступа к конфиденциальной информации;
- исключение сотрудника из резерва на выдвижение;
- другие методы (объявление взыскания, выговора и пр.).

САНКЦИИ К СОТРУДНИКАМ ОРГАНИЗАЦИИ

Основания для освобождения от должности руководителя подразделения:

- неоднократное уличение в сокрытии фактов нарушения соответствующих правил, допущенных его подчиненными;
- утечки из подразделения абсолютно конфиденциальной информации, повлекшие стратегический ущерб для организации или ее контрагентов;
- наличие регулярных замечаний со стороны службы безопасности (т.е. данный руководитель оказался не в состоянии, несмотря на принятые ранее к нему меры воздействия, обеспечить в своем коллективе требуемое отношение к информационной безопасности).

САНКЦИИ К СОТРУДНИКАМ ОРГАНИЗАЦИИ

Методы экономического характера:

- лишение или сокращение переменной части должностного оклада (доплаты, надбавки) при использовании подобных схем основной оплаты труда;
- лишение или сокращение премии по итогам квартала для конкретного сотрудника или всего коллектива структурного подразделения;
- отмена персональных или групповых социально-экономических льгот.

Методы психологического характера:

- индивидуальная беседа с руководителем или представителем службы безопасности организации;
- обсуждение допущенного сотрудником нарушения на собрании трудового коллектива подразделения.

Задание

Определите к какой категории конфиденциальной информации относятся сведения из индивидуальных досье сотрудников организации.

Домашнее задание

Сформулируйте перечень личностных качеств кандидата на трудоустройство, исключающие возможность его найма на должности, предполагающие доступ к конфиденциальной информации.

Литература

1. Алавердов А.Р. Управление кадровой безопасностью организации: учебник. – М.: Маркет ДС, 2008. – 176 с. – (Университетская серия).
2. Соломанидин В.Г., Соломанидина Т.О. Кадровая безопасность компании. – М.: Альфа-Пресс, 2011. – 688с.

Тема 5.

Противодействие угрозам имущественной безопасности организации со стороны собственного персона

УЧЕБНЫЕ ВОПРОСЫ ТЕМЫ

5.1 Имущество организации как объект защиты

5.2 Типовые причины, формы и методы реализации угроз имущественной безопасности организации с участием ее персонала

5.3 Методы противодействия угрозам имущественной безопасности организации со стороны ее персонала

5.4 Управление персоналом организации в целях обеспечения ее имущественной безопасности

СУБЪЕКТЫ УГРОЗ:

- ***конкуренты организации,*** заинтересованные в перехвате прав собственности на ее имущественные комплексы или пытающиеся ослабить ее позиции путем уничтожения элементов имущества;
- ***криминальные структуры,*** заинтересованные либо в мирном проникновении в бизнес организации, либо в отчуждении части ее имущества (перехват прав собственности, хищения в насильственной или ненасильственной форме);
- ***индивидуальные злоумышленники*** в лице хакеров, взломщиков, финансовых аферистов;
- ***клиенты или партнеры организации,*** заинтересованные в получении дополнительного дохода путем различных форм мошенничества в процессе реализации хозяйственных отношений;
- ***собственные сотрудники,*** пытающиеся улучшить свое материальное положение за счет работодателя, а также наносящие ущерб его имуществу из злого умысла или в силу собственной безответственности.

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗ

УГРОЗА РЕЙДЕРСКОГО ЗАХВАТА

с привлечением к нему нелояльных сотрудников атакуемого предприятия, задачей которых может стать:

- хищение или уничтожение документов, подтверждающих права собственности на объект захвата;
- передача рейдеру компрометирующей информации, способной стать основанием для отзыва или приостановления действия лицензии, ареста имущества, возбуждения уголовного дела, а также иных санкций со стороны государства, облегчающих передел имущественных прав;
- лжесвидетельские показания в судебных инстанциях

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗ

МЕТОДЫ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ:

- хищения в ненасильственной форме (кражи, в том числе – со взломом);
- хищения в насильственной форме (ограбление);
- хищение путем фальсификации финансовых документов;
- хищения с использованием информационных технологий.

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗ

МЕТОДЫ ХИЩЕНИЯ ИМУЩЕСТВА В МАТЕРИАЛЬНОЙ ФОРМЕ:

- хищения в ненасильственной форме;
- хищения в насильственной форме;
- перехват прав собственности;
- повреждение;
- уничтожение.

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗ

ОБЪЕКТЫ МЕЛКИХ ХИЩЕНИЙ ИМУЩЕСТВА РАБОТОДАТЕЛЯ собственными сотрудниками:

- ***в торговле*** **– предназначенные к продаже товары народного потребления;**
- ***в сфере общественного питания*** **– продукты, напитки и даже столовые приборы;**
- ***в промышленности*** **– сырье, материалы, готовая продукция, пригодные для собственного потребления работником или продажи;**
- ***в строительстве*** **– практически любые стройматериалы за исключением крупногабаритных конструкций;**
- ***на транспорте*** **– топливо и мелкие запчасти к автомобилям;**
- ***в офисах*** **– канцтовары и мелкая оргтехника**

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗЫ ИМУЩЕСТВЕННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

СО СТОРОНЫ КОНКУРЕНТОВ:

- изъятие или фальсификация документов, подтверждающих право собственности;
- проведение заведомо убыточных операций;
- уничтожение имущественных комплексов (например, поджог офиса или склада с продукцией).

СО СТОРОНЫ НЕДОБРОСОВЕСТНЫХ КЛИЕНТОВ ИЛИ ПАРТНЕРОВ:

- изъятие или фальсификация документов, подтверждающих право собственности организации на отгруженную продукцию или переданное в аренду имущество;
- заключение невыгодной или прямо убыточной для организации сделки купли – продажи, аренды и т.п., а также скрытое лоббирование ее.

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗЫ ИМУЩЕСТВЕННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

СО СТОРОНЫ КРИМИНАЛЬНЫХ СТРУКТУР:

- кражи;
- ограбления;
- изъятие или фальсификация документов, подтверждающих право собственности;
- умышленное уничтожение имущества;
- мошеннические финансовые операции.

СО СТОРОНЫ ИНДИВИДУАЛЬНЫХ ЗЛОУМЫШЛЕННИКОВ:

- кражи денежных средств и товарно-материальных ценностей;
- мошеннические финансовые операции;
- обеспечение возможности доступа к управлению финансовыми операциями с использованием информационных технологий.

ФОРМЫ РЕАЛИЗАЦИИ УГРОЗЫ ИМУЩЕСТВЕННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ со стороны собственных сотрудников

- мелкие хищения товарно-материальных ценностей организации (от канцтоваров до относительно дешевой готовой продукции);
- крупные хищения товарно-материальных ценностей организации (от дорогостоящей готовой продукции до производственного оборудования), совершаемые обычно в сговоре с коллегами или сторонними злоумышленниками;
- хищения наличных денежных средств;
- хищения наличных и безналичных денежных средств путем фальсификации финансовых документов;
- хищение денежных средств с использованием информационных технологий;
- нанесение организации ущерба в результате коррупции при заключении хозяйственных договоров и контрактов;
- умышленное повреждение или уничтожение имущества организации (саботаж);
- неумышленное повреждение или уничтожение имущества организации (преступная небрежность).

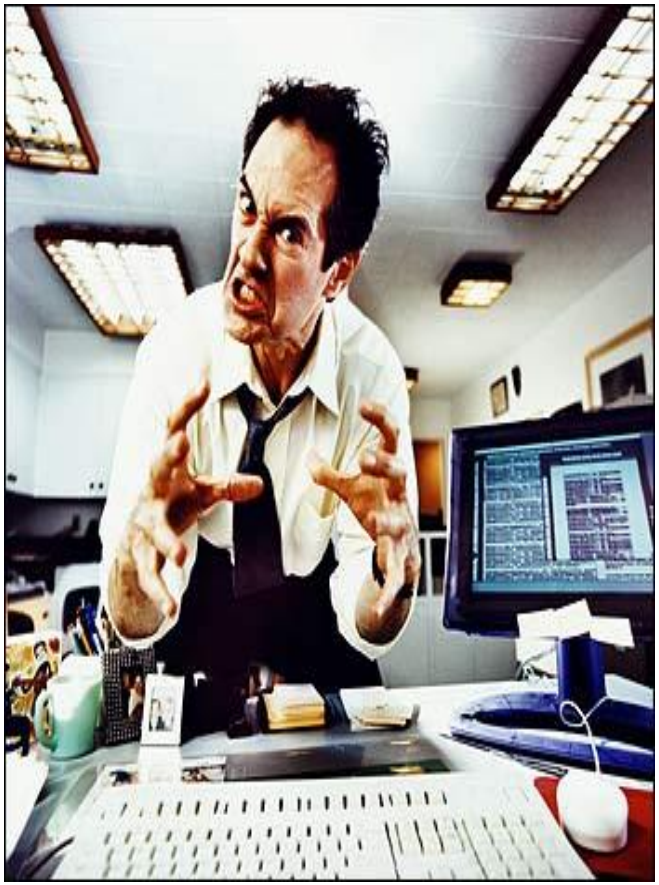
МЕТОДЫ ПРОТИВОДЕЙСТВИЯ УГРОЗЕ МЕЛКИХ ХИЩЕНИЙ ЛИКВИДНЫХ ТОВАРНО-МАТЕРИАЛЬНЫХ ЦЕННОСТЕЙ

- **строгий учет хранения и использования товарно-материальных ценностей;**
- **регулярные инвентаризации;**
- **использование эффективных технических и организационных методов защиты товарно-материальных ценностей;**
- **использование механизма индивидуальной и коллективной (бригадной) полной материальной ответственности**

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ УГРОЗЕ КОРРУПЦИИ СО СТОРОНЫ ДОЛЖНОСТНЫХ ЛИЦ ОРГАНИЗАЦИИ:

- специальные процедуры отбора кандидатов на замещение соответствующих должностей;
- использование «коллегиального подхода» при подготовке решений о заключении соответствующих договоров;
- независимая экспертиза проектов заключаемых договоров
- текущий контроль доходов соответствующих должностных лиц;
- специальные методы мотивации соответствующих должностных лиц

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ УГРОЗЕ ХИЩЕНИЙ В ПРОЦЕССЕ УПРАВЛЕНИЯ ЭЛЕКТРОННЫМИ ПЛАТЕЖАМИ И РАСЧЕТАМИ:



- использование специальных программных продуктов, препятствующих несанкционированному доступу к управлению платежами и расчетами в электронной форме и регулярное их обновление;
- специальные процедуры контроля над деятельностью сотрудников, допущенных к управлению такими расчетами;
- использование дополнительных услуг обслуживающего банка в области обеспечения безопасности финансовых расчетов в электронной форме

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ УГРОЗЕ КРУПНЫХ ХИЩЕНИЙ СОТРУДНИКАМИ ДЕНЕЖНЫХ СРЕДСТВ И ИНОГО ИМУЩЕСТВА РАБОТОДАТЕЛЯ

- строгий учет хранения и использования денежных средств и других ликвидных активов;
- регулярное проведение внутренних и внешних (независимых) аудиторских проверок;
- использование эффективных технических и организационных методов защиты денежных средств и других ликвидных активов;
- текущий контроль доходов соответствующих должностных лиц;
- использование механизма полной материальной ответственности

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ УГРОЗЕ ПОВРЕЖДЕНИЯ ИЛИ УНИЧТОЖЕНИЯ СОТРУДНИКАМИ ИМУЩЕСТВА РАБОТОДАТЕЛЯ

ПРЕДОТВРАЩЕНИЕ УМЫШЛЕННЫХ ДЕЙСТВИЙ:

- использование механизма полной материальной ответственности;
- текущий контроль лояльности персонала

ПРЕДОТВРАЩЕНИЕ НЕ УМЫШЛЕННЫХ ДЕЙСТВИЙ:

- использование механизма полной материальной ответственности;
- использование специальных технических средств защиты;
- использование специальных процедур допуска к работе

ОСОБЕННОСТИ В ОРГАНИЗАЦИИ ОБУЧЕНИЯ ПЕРСОНАЛА:

- необходимость организации специального технического обучения части сотрудников, уменьшающего вероятность реализации угрозы в форме неумышленного повреждения имущества работодателя;

- необходимость специального обучения сотрудников службы безопасности технике отражения угроз имущественной безопасности организации, осуществляемых насильственными методами.

ОСОБЕННОСТИ В ОРГАНИЗАЦИИ КОНТРОЛЯ НАД ПЕРСОНАЛОМ:

- **включение в число субъектов контроля финансовой службы (в корпорациях – кроме того, и специальной службы внутреннего аудита), а также всех материально-ответственных лиц;**
- **использование разнообразных форм и методов финансового контроля;**
- **использование технологий инвентаризации и других форм контроля над сохранностью имущества в материальной форме;**
- **использование независимых экспертов для проверки заключаемых контрактов и договоров с позиции их экономической эффективности для организации;**
- **большее внимание к обеспечению организации электронными и техническими средствами контроля над сохранностью имущества.**

ОСОБЕННОСТИ В ОРГАНИЗАЦИИ МОТИВАЦИИ ПЕРСОНАЛА

В области позитивной мотивации:

- активное использование форм основной и дополнительной оплаты труда, снижающих вероятность финансовых и иных злоупотреблений со стороны менеджеров и специалистов (механизм участия в прибыли, комиссионные процентом от суммы контракта и т.п.);
- использование механизмов внутрихозяйственного расчета и внутрихозяйственной аренды для предотвращения индивидуальных и групповых хищений товарно-материальных ценностей.

ОСОБЕННОСТИ В ОРГАНИЗАЦИИ МОТИВАЦИИ ПЕРСОНАЛА

В области специальных санкций:

- лучшие возможности для возмещения прямого ущерба, нанесенного сотрудниками, имеющими должностной статус «материально ответственного лица»;
- лучшие возможности для привлечения сотрудников, виновных в хищениях имущества работодателя, не только к административной, но и к уголовной ответственности.

Задание

Определите элементы имущества организации как приоритетные объекты защиты применительно к следующим сферам бизнес деятельности: банковский сектор, сфера торговли и услуг, жилищное строительство, пищевая промышленность.

Домашнее задание

Раскройте принцип действия и сформулируйте преимущества механизма полной коллективной материальной ответственности как универсального метода борьбы с мелкими хищениями сотрудниками предприятия его имущества..

Литература

1. Алавердов А.Р. Управление кадровой безопасностью организации: учебник. – М.: Маркет ДС, 2008. – 176 с. – (Университетская серия).
2. Соломанидин В.Г., Соломанидина Т.О. Кадровая безопасность компании. – М.: Альфа-Пресс, 2011. – 688с.

БЛАГОДАРЮ ЗА ВНИМАНИЕ!